IBM Cloud Application Performance Management
Junio de 2019

Guía del usuario

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 1551.

Esta edición se aplica a la versión de junio de 2019 de IBM® Cloud Application Performance Management y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Contenido

Capítulo 1. Novedades

En el último release hay características, prestaciones y cobertura nuevas disponibles.

- Para obtener información sobre la versión del agente en cada release o renovación, consulte "Historial de cambios" en la página 52.

Diciembre de 2019

Nuevo agente

Agente de MariaDB

Monitoring Agent for MariaDB ofrece un punto central de la gestión para la aplicación o el entorno de MariaDB. El software proporciona medios completos para recopilar la información necesaria para detectar problemas de forma precoz y evitarlos. La información está estandarizada en todo el sistema. Puede supervisar varios servidores desde una única consola. Mediante Monitoring Agent for MariaDB, puede recopilar y analizar fácilmente información específica de MariaDB.
Para obtener información sobre la configuración del agente después de la instalación, consulte "Configuración de la supervisión de MariaDB" en la página 502

Soporte de plataforma ampliado para agentes

Ahora se da soporte a los siguientes agentes y plataformas:

Solaris X86-64

- Agente de Oracle Database
- Agente de WebLogic

Mejoras en los agentes

Agente de Cassandra

Se han añadido dos nuevos atributos denominados `Nombre de host de agente` y `Nombre de instancia de agente` en los grupos de atributos `Detalles de clúster`, `Estadísticas de nodo` y `Detalles de espacio de claves`.

Agente de Db2

Se ha añadido soporte para supervisar `SQL en ejecución actual`.

Agente de IBM Integration Bus

Se han añadido dos nuevos widgets de grupo, `Conexiones de cliente TCPIP` y `Conexiones de servidor TCPIP` en la página `Estado del servidor de integración - Detalle`.

Internet Service Monitoring

- Se han añadido dos nuevas variables del panel de configuración:
  - *Activo*: para seleccionar un estado para el elemento de perfil como activo o inactivo.
  - *sniServerName*: indica el nombre del host/servidor para el que se necesita un certificado del servidor web habilitado para SNI.
- **Valores predeterminados** en la ficha **Validación de datos** para los supervisores HTTP, HTTPS y DNS ahora se pueden editar
- El agente ahora da soporte al carácter & en el campo **página** para los supervisores HTTP y HTTPS
- Al agente ahora da soporte a caracteres daneses en el campo **regex** de los supervisores HTTP y HTTPS

  Nota: Establezca el entorno local en da_DK en la plataforma Linux antes de la instalación del agente para utilizar esta característica

Agente de Microsoft Active Directory

- Se ha añadido un nuevo widget denominado Detalles de KCC en la página Visión general de estado.
- Se han añadido los siguientes grupos de atributos nuevos en la ficha Detalles de atributo:
  - Servicios de directorio
  - Kerberos Consistency Checker
  - Centro de distribución de claves Kerberos
  - Proveedor de servicio de nombres
  - Servicio de directorio de Exchange

Agente de Microsoft .NET

Se ha añadido un nuevo atributo denominado Nombre de solicitud en el grupo de atributos Detalles de llamadas a base de datos. Este atributo visualiza el nombre de la solicitud que activa la consulta de base de datos.

Agente de Microsoft Exchange Server

- Se ha añadido un nuevo widget denominado Recepción de SMTP de transporte en la página Visión general del estado.
- Se han añadido los siguientes grupos de atributos nuevos en la ficha Detalles de atributo:
  - AB de MS Exchange
  - Procesos de MS Exchange ADAccess
  - Memorias caché de MS Exchange ADAccess
  - Controladores de dominio de MS Exchange ADAccess
  - Descubrimiento de bosque de MS Exchange ADAccess

Agente de Microsoft Hyper-V Server

Se ha añadido soporte para Windows Server 2019.

Agente de Microsoft IIS

- Se han añadido nuevos widgets de grupo:
  - Estadísticas de memoria principal del sistema
  - Servidor IIS - Uso de memoria asignado
  - Servidor IIS - Uso de CPU asignado
  - Detalles de proceso de trabajador
  - Gestión de la memoria .Net
- En cada nombre de agrupación de aplicaciones en el widget de grupo Detalles de proceso de trabajo, se crea una página que muestra la tendencia histórica de solicitudes procesadas por segundo, Tiempo transcurrido, Solicitudes en cola, Utilización de memoria y CPU.
- En cada nombre de agrupación de aplicaciones en el widget de grupo Gestión de la memoria .Net se añade una ventana emergente que muestra la tendencia histórica del tiempo de porcentaje en la recogida de basura.

Agente de Microsoft SharePoint Server

- Se ha añadido un nuevo grupo de atributos denominado Trace_Log que proporciona la información de registros de gravedad alta.
- Se han añadido dos nuevos widgets de grupo denominados Detalles de registro de rastreo y Recuento del registro de rastreo de la última 1 hora en la página Visión general para visualizar los detalles de los 100 sucesos de registro de rastreo recientes y el recuento de la última 1 hora de registros de rastreo de nivel superior e inesperados.

Agente de MySQL

El agente recopila datos de forma coherente después del reinicio del servidor.

Agente de NetApp Storage
El agente ahora muestra la lista exacta de Qtress que se correlacionan con el volumen.

Agente de PostgreSQL
El agente ahora da soporte al servidor PostgreSQL versión 12.

Agente de Supervisión de tiempo de respuesta

- Se ha añadido un nuevo parámetro de configuración KT5AARIPTOUSERID. Le permite guardar la dirección IP de cliente en la propiedad Nombre de usuario en los datos sin formato AAR. De forma predeterminada, se establece como NO. Para cambiar el valor, es necesario reiniciar el Agente de Supervisión de tiempo de respuesta.
  - KT5AARIPTOUSERID=NO: si el valor es NO, el agente de Agente de Supervisión de tiempo de respuesta guardará el nombre de usuario de la transacción en la propiedad userID de AAR.
  - KT5AARIPTOUSERID=YES: si el valor es YES, el Agente de Supervisión de tiempo de respuesta guardará la dirección IP del origen de la transacción en la propiedad userID de AAR.
- El Agente de Supervisión de tiempo de respuesta ahora da soporte a la especificación del valor KT5AARIPTOUSERID en la configuración silenciosa.
- El título del widget de grupo existente Peor por usuario - 5 principales se ha cambiado a Peor por usuario - 20 principales. El widget de grupo se ha cambiado para mostrar los 20 usuarios principales con el mayor porcentaje de anomalías de transacción durante el periodo seleccionado.

VMware

- El agente ahora da soporte a la captación de la dirección IP o el nombre de host de vCenter desde la llamada a la API de vSphere, en lugar de mostrar Dirección configurada como lo hace en el panel de configuración. El usuario puede activar esta característica estableciendo el distintivo en el entorno de agente en Y. Por ejemplo, KVM_RETRIEVE_HOSTNAME_FROM_API=Y.
- Ahora se puede dar un límite al recuento de reintentos para restringir los intentos de conexión con el origen de datos. Por ejemplo, KVM_DATA_PROVIDER_CONNECTION_RETRY_COUNT=1000, al añadir esta variable en el archivo de entorno de agente se podrá un bloqueo en el recuento de reintentos de conexión en caso de anomalía de conexión con vCenter. 1000 indica que el agente intentará hasta 1000 intentos de conexión fallidos subsiguientes y luego hará caer el proceso del proveedor de datos con un mensaje de registro NO MÁS INTENTOS DE CONEXIÓN; DETENIENDO LA RECOPILACIÓN DE DATOS, PARA REANUDAR LA SUPERVISIÓN REINICIE EL AGENTE. PARA TENER MÁS INTENTOS DE CONEXIONES, RESTABLEZCA EL VALOR DE LA VARIABLE KVM_DATA_PROVIDER_CONNECTION_RETRY_COUNT. El valor predeterminado para reintentar los intentos de conexión es 6, el usuario puede establecer el umbral deseado según el requisito.
- El agente da soporte a la configuración del tamaño de almacenamiento dinámico específico de la instancia para utilizar eficientemente la memoria asignada en el sistema. Por ejemplo, KVM_CUSTOM_JVM_ARGS= -Xmx512m, si se establece esta variable en el archivo de entorno de la instancia significará que la instancia se ha configurado para utilizar 512 MB de memoria de almacenamiento dinámico. El tamaño se puede cambiar en función del recuento total de objetos vCenter que una instancia esté supervisando.

Septiembre de 2019

Soporte de plataforma ampliado para agentes
Ahora se da soporte a los siguientes agentes y plataformas:

Solaris X86-64

- Agente de Db2
- Agente de SAP
- Agente de Sybase

- Agente de sistema operativo UNIX
- Agente de WebSphere Applications
- Agente de WebSphere MQ
- Agente de IBM Integration Bus

RHEL on x86-64 (64 bits)

- Agente de Internet Service Monitoring
- Agente de Microsoft SQL Server
- Agente de Sybase

RHEL on POWER Little Endian (ppc64le)

- Agente de RabbitMQ

Mejoras en los agentes

Agente de Db2

- El agente da soporte ahora al servidor de Db2 versión 11.5.

Agente de Hadoop

- Se ha añadido al panel de configuración un nuevo parámetro de configuración **`Nombre de clúster exclusivo`**, que es un nombre exclusivo para el clúster de Hadoop que indica su versión y tipo.
- Ahora, el agente de Hadoop muestra el elemento de visualización para los umbrales creados en los servicios de Ambari.
- Ahora, el agente de Hadoop da soporte a la supervisión del servicio de Streaming Analytics Manager en el clúster de Hadoop.
- Ahora, el agente de Hadoop da soporte a la supervisión del servicio de registro de esquema en el clúster de Hadoop.

Agente de HTTP Server

- El agente da soporte ahora al servidor HTTP de Oracle en Solaris Sparc.

Internet Service Monitoring

- El agente da soporte ahora a IBM Tivoli Netcool/OMNIbus.
- El agente se ha mejorado para suprimir perfiles de los perfiles existentes y cambiar el nombre de los perfiles existentes.

Agente de MongoDB

- El agente da soporte ahora a la base de datos MongoDB versión 4.x.

Agente de MySQL

- Se ha añadido el atributo FQDN para Disponibilidad de aplicaciones en la sección Ayuda.
- Visualización de ayuda contextual fija para el parámetro de configuración de agente Dirección IP.
- Se han añadido los siguientes atributos nuevos para la supervisión en IBM Cloud App Management.
  - Información de tamaño de base de datos
  - Información de errores
  - Recuento de bloqueos de instancia de base de datos
  - Detalles de conexión del usuario
  - Detalles de lista de procesos
  - Información de sucesos

Agente de PostgreSQL

- Se han añadido dos nuevas situaciones denominadas `Deadlocks_Count_Crit` y `Deadlocks_Count_Warn` para supervisar el número de puntos muertos de una base de datos, lo cual ayudará a corregir el problema exacto de los puntos muertos.
- Se ha añadido un nuevo grupo de atributos denominado `Deadlocks_Info` para comprobar los detalles del punto muerto.

Agente de Sybase

- Se ha añadido el atributo FQDN para Disponibilidad de aplicaciones en la sección Ayuda.

Agente de Synthetic Playback

- Ahora se da soporte a Firefox V68.0 ESR.
- Las configuraciones de proxy del sistema, proxy de PAC y sin proxy están ahora soportadas.

Agente de Tomcat

- El agente se ha mejorado con métricas y vistas de interfaz de usuario para supervisar el uso de la agrupación de memoria de almacenamiento dinámico/no de almacenamiento dinámico para la JVM.
- El agente se ha mejorado con métricas y vistas de interfaz de usuario para la supervisión de hebras y la información de carga de clases para la JVM.
- La interfaz de usuario del agente muestra ahora el FQDN en la vista Información del servidor.

Agente de sistema operativo UNIX

- El agente se ha actualizado con la característica de scripts personalizados. Se pueden utilizar scripts de shell, scripts PERL y otros tipos de scripts.

Agente de VMware VI

- Se ha añadido un nuevo campo de configuración denominado **KEY_STORE_PASSWORD**. Permite a los usuarios configurar el agente con la nueva contraseña de almacén de claves para el JRE del agente.

Junio de 2019

Soporte de plataforma ampliado para agentes

Ahora se da soporte a los siguientes agentes y plataformas:

Red Hat Enterprise Linux (RHEL) 8

Los siguientes agentes y recopiladores de datos ahora dan soporte a RHEL 8. Antes de instalar agentes en RHEL 8, asegúrese de leer la sección "Sistemas operativos específicos" en la página 134 de "Preinstalación en sistemas Linux" en la página 134.

RHEL 8 on x86-64 (64 bits)

- Agente de Cassandra
- Agente de Cisco UCS
- Agente de DataPower
- Agente de DataStage
- Agente de Db2
- Agente de Hadoop
- Agente de HTTP Server
- Integration Agent for Netcool/OMNIbus
- agente Internet Service Monitoring
- Recopilador de datos de J2SE
- Agente de Linux KVM

- Agente de sistema operativo Linux
- Agente de MongoDB
- Agente de MQ Appliance
- Agente de MySQL
- Agente de NetApp Storage
- Recopilador de datos de Node.js
- Agente de PHP
- Recopilador de datos de Python
- Agente de PostgreSQL
- Agente de RabbitMQ
- Agente de Supervisión de tiempo de respuesta
- Agente de Ruby
- Agente de SAP
- Agente de SAP HANA Database
- Agente de SAP NetWeaver Java™ Stack
- Agente de Sterling Connect Direct
- Agente de Sterling File Gateway
- Agente de Sybase
- Agente de Tomcat
- Agente de VMware VI
- Agente de WebSphere Applications
- Agente de WebSphere MQ

RHEL 8 on System z

- Agente de Db2
- Agente de Hadoop
- Agente de sistema operativo Linux
- Agente de MySQL
- Recopilador de datos de Node.js
- Recopilador de datos de Python
- Agente de Supervisión de tiempo de respuesta
- Agente de WebSphere Applications
- Agente de WebSphere MQ

RHEL 8 on POWER Little Endian (ppc64le)

- Agente de Db2
- Agente de Hadoop
- Recopilador de datos de J2SE
- Agente de sistema operativo Linux
- Agente de MySQL
- Recopilador de datos de Node.js
- Agente de SAP NetWeaver Java Stack
- Agente de WebSphere Applications
- Agente de WebSphere MQ

Solaris Sparc 10 y 11

- Agente de JBoss
- Agente de Oracle Database
- Agente de WebLogic

Windows Server 2019

- Agente de WebSphere Applications

Mejoras en los agentes

Agente de Hadoop

- El Agente de Hadoop da soporte ahora a la supervisión del servicio Ambari HDF 3.3 (con HDP 3.1.0) Big SQL 6.0.
- El Agente de Hadoop da soporte ahora a la plataforma SUSE Linux Enterprise Server (SLES) 15 on x86-64.

Agente de HMC Base
El Agente de HMC Base da soporte a HMC V9.1.

Integration Agent for Netcool/OMNIbus
El agente se ha actualizado para dar soporte a Red Hat Enterprise Linux (RHEL) 8 y SUSE Linux Enterprise Server (SLES) 15

Agente de Internet Service Monitoring
El agente tiene ahora el supervisor de Service Assurance Agent, que supervisa los análisis de Cisco Service Assurance Agent.

Agente de Microsoft IIS
El agente se ha mejorado con el suministro de tolerancia al servidor Windows 2019. Esta mejora muestra los datos del sitio FTP para el agente que está instalado en el servidor Windows 2019.

Agente de MongoDB
El agente da soporte ahora a la plataforma Red Hat Enterprise Linux (RHEL) 8 on x86-64 (64 bits).

Recopilador de datos de Python ifix02
El recopilador de datos da soporte ahora a Django 1.10 y superior.

Agente de SAP

El Agente de SAP da soporte ahora a las plataformas siguientes:

- Red Hat Enterprise Linux (RHEL) 8 on x86-64 (64 bits)
- SAP NetWeaver Application Server 7.52 (SAP Basis 752)

Agente de SAP HANA Database

El Agente de SAP HANA Database se ha mejorado con las características siguientes:

- Se ha añadido el nombre de host al nodo Subnodo :HDB del Agente de SAP HANA Database para su identificación exclusiva.
- El agente da soporte ahora a la arquitectura de escalado.
- Plataformas Red Hat Enterprise Linux (RHEL) 8 on x86-64 (64 bits) y Linux ppc64le.
- Plataforma SUSE Linux Enterprise Server (SLES) 15 on x86-64 (64 bits).
- Se ha añadido un nuevo atributo de host recortado (Host Trimmed) al grupo de atributos Base de datos del sistema.

Agente de SAP NetWeaver Java Stack

El Agente de SAP NetWeaver Java Stack da soporte a las plataformas siguientes:

- Red Hat Enterprise Linux (RHEL) 8 on x86-64 (64 bits)
- SUSE Linux Enterprise Server (SLES) 15 on x86-64 (64 bits)
- Windows Server 2019 DE y SE

- Windows Server 2016 DE y SE

Agente de Synthetic Playback

- Da soporte al script .side grabado por Selenium IDE 3.2.X, 3.3.X o 3.5.X
- Soporta la reproducción mediante Firefox ESR 60.5.1
- Da soporte a los mandatos **`wait`**, **`flow control`** y **`linkText locator type`** de Selenium IDE

Agente de Skype for Business Server

El Agente de Skype for Business Server se ha mejorado con las características siguientes:

- El agente da soporte ahora a Skype for Business Server 2019.
- Se han añadido dos nuevos widgets de grupo, `Base de datos – Solicitudes reguladas (DBStore)` y `Base de datos – Solicitudes reguladas (SHAREDDBStore)` a la página Visión general, que muestran el número de solicitudes reguladas por Skype for Business Server debido a la alta latencia de la cola de base de datos para DBstore y DBstore compartido.

Escáner de requisitos previos

Ahora, el mandato **`IGNORE_PRECHECK_WARNING`** está disponible como una alternativa al mandato **`SKIP_PRECHECK`**. Para obtener más información, consulte "Eludir la exploración de requisitos previos" en la página 150.

Mejora de la documentación

Se ha creado una página para ayudarle a encontrar rápidamente la información de versión y el historial de cambios de cada agente y recopilador de datos. Consulte "Historial de cambios" en la página 52.

Marzo de 2019

Soporte de plataforma ampliado para agentes

Ahora se da soporte a los siguientes agentes y plataformas:

Windows Server 2019

- Agente de Cassandra
- Agente de DataStage
- Agente de Db2
- Agente de Hadoop
- Internet Service Monitoring
- Agente de Microsoft Active Directory
- Agente de Microsoft Cluster Server
- Agente de Microsoft IIS
- Agente de Microsoft Exchange Server
- Agente de Microsoft SQL Server
- Agente de MySQL
- Agente de PostgreSQL
- Agente de RabbitMQ
- Agente de SAP
- Agente de SAP HANA Database
- Agente de Sybase
- Agente de Tomcat

- Agente de sistema operativo Windows

Solaris SPARC 10 y 11

- Agente de Db2
- HTTP Server
- Agente de MySQL
- Agente de SAP
- Agente de Sybase
- Agente de sistema operativo UNIX
- Agente de WebSphere Applications

Monitoring Agent for Cassandra

El Agente de Cassandra se ha mejorado con las características siguientes:

- Se ha añadido soporte para el sistema operativo Windows Server 2019.
- Se ha añadido un registro detallado para la resolución de problemas.

Monitoring Agent for Db2

El agente de Db2 se ha mejorado con las características siguientes:

- El agente de Db2 da soporte ahora a Windows Server 2019.
- El agente de Db2 da soporte ahora a las plataformas Solaris SPARC 10/11.

Monitoring Agent for Hadoop

El Agente de Hadoop se ha mejorado con las características siguientes:

- Se ha añadido soporte para supervisar los clústeres de Hadoop BigInsights, Hortonworks y Cloudera habilitados para SSL.
- Se ha añadido soporte para probar la conexión al clúster de Hadoop habilitado para SSL.
- Se ha añadido soporte del sistema operativo Windows Server 2019 (Ediciones Datacenter y Standard).
- Se ha añadido soporte para la supervisión de la oferta de Hadoop: Cloudera 6.1.1 (CDH 6.1.1).
- Se ha añadido soporte para la supervisión de la oferta de Hadoop: Hortonworks 3.1.0 (HDP 3.1.0).

Monitoring Agent for IBM Integration Bus

El Agente de IBM Integration Bus se ha mejorado con la característica siguiente:

- Se ha añadido soporte de tolerancia para supervisar IBM App Connect Enterprise V11. Para obtener más información, consulte “Configuración del Agente de IBM Integration Bus” en la página 287.

Monitoring Agent for Microsoft Internet Information Services

El Agente de Microsoft IIS da soporte ahora al sistema operativo Windows Server 2019.

Monitoring Agent for InfoSphere DataStage

El Agente de DataStage se ha mejorado con las características siguientes:

- Se ha añadido soporte para el sistema operativo Windows Server 2019.
- Se ha añadido un tiempo de espera de consulta a las consultas de recopilación de datos para obtener un mejor rendimiento del agente.

Monitoring Agent for Microsoft Active Directory

El Agente de Microsoft Active Directory se ha mejorado con las características siguientes:

- Se ha añadido soporte para Windows Server 2019.
- Se ha añadido un nuevo grupo de atributos `AD_Services_Status` que proporciona el estado de servicios relacionados con el servidor de Active Directory.
  En función del estado de los servicios, determina el estado del servidor de Active Directory.

- Se ha añadido una nueva situación AD_Server_Status que supervisa el estado del servidor de Active Directory.
- Se ha añadido un nuevo grupo de atributos Root_Directory_server que proporciona la versión activa y el nombre del sistema operativo supervisado.

Monitoring Agent for Microsoft Cluster Server

El Agente de Microsoft Cluster Server se ha mejorado con las características siguientes:

- Se ha añadido soporte para el sistema operativo Windows Server 2019.
- Se ha añadido el atributo CLUSTER_SERVICE_VERSION.

Monitoring Agent for Microsoft Exchange Server

El Agente de Microsoft Exchange Server se ha mejorado con las características siguientes:

- Se ha añadido soporte para MS Exchange Server 2019.
- Se ha añadido un nuevo grupo de atributos MSExchange MAPIoverHTTP que proporciona información sobre las estadísticas de MAPI a través del protocolo HTTP.

Monitoring Agent for Internet Services

El agente de Internet Service Monitoring se ha mejorado con las características siguientes:

- Se ha añadido soporte para los supervisores LDAP, NTP, NNTP, SOAP, SNMP, SIP, RTSP, RPING, RADIUS y TFTP.
- Se ha añadido soporte para el sistema operativo Windows 2008 R2 Server y Windows Server 2019.

Monitoring Agent for Microsoft SQL Server

El Agente de Microsoft SQL Server da soporte ahora a Windows Server 2019.

Monitoring Agent for MySQL

El Monitoring Agent for MySQL se ha mejorado con las características siguientes:

- Se ha añadido soporte para Windows Server 2019.
- Se ha añadido soporte para las plataformas Solaris SPARC 10/11.
- Se ha añadido la posibilidad de establecer propiedades adicionales para la conexión JDBC iniciada por el agente con el servidor MySQL.

Monitoring Agent for PostgreSQL

El Agente de PostgreSQL da soporte ahora al sistema operativo Windows Server 2019.

Monitoring Agent for RabbitMQ

El Agente de RabbitMQ da soporte ahora al sistema operativo Windows Server 2019.

Monitoring Agent for Skype for Business Server

El Agente de Skype for Business Server se ha mejorado con las características siguientes:

- Se ha añadido soporte para el sistema operativo Windows Server 2019.
- Se ha añadido un nuevo grupo de atributos denominado KQL_Server para visualizar la información relacionada con el producto Skype for Business Server.
- Se ha añadido una nueva situación denominada Skype_Server_Down para supervisar el estado de Skype for Business Server basándose en el estado de los servicios de conferencia de IM y de componente frontal del servidor.

Monitoring Agent for SAP Applications

El Agente de SAP se ha mejorado con las características siguientes:

- Se ha añadido la característica de contraseña sensible a mayúsculas y minúsculas para el usuario de aplicación que se utiliza entre el agente de SAP y el servidor de SAP.

- Se ha añadido soporte para el sistema operativo Windows Server 2019 (Ediciones Datacenter y Standard).
- Se ha añadido soporte para ver los trabajos de larga ejecución que están presentes en el sistema SAP durante más de 24 horas.
- Se ha mejorado el rendimiento del módulo de función /IBMMON/ITM_MAIALRT_INX.
- Se ha añadido soporte para los sistemas operativos Solaris v10 y v11 SPARC
- Se ha añadido una característica de recorte al nombre de host de SAP para que coincida con el límite máximo de 32 caracteres del Nombre de sistema gestionado.

Monitoring Agent for SAP HANA Database

El Agente de SAP HANA Database se ha mejorado con las características siguientes:

- Se ha añadido soporte para descubrir las bases de datos de arrendatario cuando el nombre de base de datos de arrendatario y el SID del sistema HANA son iguales.
- Se ha añadido soporte para el sistema operativo Windows Server 2019 (Ediciones Datacenter y Standard).

Monitoring Agent for Sybase Server

El Agente de Sybase se ha mejorado con las características siguientes:

- Se ha añadido soporte para Windows Server 2019.
- Se ha añadido soporte para las plataformas Solaris SPARC 10/11.
- Se ha mejorado la consulta de Sybase para obtener una mejor simultaneidad y reducir el bloqueo.

Monitoring Agent for Tomcat

El Agente de Tomcat da soporte ahora al sistema operativo Windows Server 2019 (Ediciones Datacenter y Standard).

Monitoring Agent for UNIX OS

El Agente de sistema operativo UNIX se ha mejorado con la característica siguiente:

- Se ha añadido soporte para Solaris SPARC 10 y 11.

Monitoring Agent for VMware VI

El Agente de VMware VI se ha renovado para ignorar los valores de indisponibilidad (-1) al visualizar la tendencia de promedio en el gráfico para todos los gráficos de varias líneas.

Monitoring Agent for WebSphere Applications

El Agente de WebSphere Applications se ha mejorado con las características siguientes:

- Se ha añadido soporte para Solaris SPARC 10 y 11.
- Se ha añadido soporte para la supervisión de WebSphere® Extreme Scale. Puede configurar la supervisión para una o varias zonas de Extreme Scale, bajo el nodo de cualquier servidor que pertenezca a la zona o zonas. Puede profundizar para visualizar información para diferentes servidores, conjuntos de correlaciones y particiones dentro de la zona o zonas. Para obtener más información, consulte "Configuración del Agente de WebSphere Applications para supervisar WebSphere Extreme Scale" en la página 954.

Monitoring Agent for WebSphere MQ

El Agente de WebSphere MQ se ha mejorado con las características siguientes:

- Se ha añadido soporte para SLES 15 xLinux.
- Se ha añadido soporte para recopilar estadísticas para el gestor de colas y visualizar los datos recopilados. Para obtener más información, consulte "Habilitación de la supervisión de estadísticas de cola para el gestor de colas de IBM MQ" en la página 975.

Mejoras de recopiladores de datos

Recopilador de datos de J2SE

El Recopilador de datos de J2SE se ha mejorado con las características siguientes:

- Se ha añadido soporte para OpenJDK versiones 9, 10 y 11.
- Se ha añadido soporte del sistema operativo Windows Server 2019 (Ediciones Datacenter y Standard).
- Se ha añadido una función para descubrir automáticamente las clases y métodos específicos de la aplicación J2SE para la supervisión de rastreo de transacciones y de datos de diagnóstico.

Selenium IDE 3.2.X y 3.3.X para scripts sintéticos

Si la suscripción incluye el complemento IBM Website Monitoring on Cloud, las versiones 3.2X.X y 3.3.X de Selenium IDE están ahora soportadas; los scripts y suites de pruebas se guardan en el formato `.side` en lugar del formato `.html` utilizado por las versiones anteriores de Selenium IDE. Si tiene scripts `.html` preexistentes, puede seguir utilizándolos. En algunos casos, es posible que desee editar los scripts `.html` o volver a grabarlos en el nuevo formato `.side`.

Para obtener más información, consulte estos subtemas de "Gestión de transacciones sintéticas y sucesos con Website Monitoring" en la página 1061: "Grabación de scripts sintéticos" en la página 1062, "Estructuración de scripts complejos" en la página 1065 y "Actualización de scripts desde versiones anteriores de Selenium IDE" en la página 1066.

Diciembre de 2018

Nuevo agente

Monitoring Agent for IBM Cloud

Monitoring Agent for IBM Cloud recopila inventario de máquina virtual y métricas de la cuenta IBM Cloud (Softlayer). Utilice el Agente de IBM Cloud para realizar el seguimiento de cuántos dispositivos virtuales se han configurado y se están ejecutando en IBM Cloud. Puede ver qué recursos se asignan a cada dispositivo virtual en la página del panel de instrumentos detallada, que también muestra información como el centro de datos en el que se encuentra un dispositivo, el sistema operativo y el ancho de banda de red público proyectado para el mes.

Mejoras en los agentes

Monitoring Agent for Cassandra

El agente de Cassandra se ha mejorado con las siguientes características:

- Se ha añadido un nuevo umbral denominado `Cassandra_Cluster_Down` que supervisa el estado de la instancia supervisada.
- Se ha añadido soporte para el sistema operativo Ubuntu 18.04.
- Se ha añadido soporte para la plataforma SUSE Linux Enterprise Server 15.

Monitoring Agent for Db2

El agente de Db2 se ha mejorado con las características siguientes:

- El agente de Db2 da soporte ahora a las prestaciones de supervisión de HADR para varios sistemas en espera.
- El agente de Db2 da soporte ahora al nuevo valor `Stopped` (Detenido) para el atributo Estado de base de datos.
  El estado `Detenido` indica que la base de datos no está activa y que tiene cero conexiones activas mientras está en buen estado y lista para aceptar nuevas conexiones.
- Se ha añadido un nuevo widget `Información de servidor Db2` para visualizar detalles del servidor Db2.
- Se ha añadido la nueva página `Estado de HADR – Bases de datos locales` para mostrar la información sobre bases de datos de asociados en los siguientes nuevos widgets:
  - `Detalles de bases de datos HADR` es el widget de tabla que visualiza valores de atributos importantes para la base de datos asociada.
  - `Intervalo de registro (Historial)` es el widget gráfico que visualiza la tendencia de intervalo del registro versus tiempo.

  - Estado de distintivo en espera es el widget de tabla que visualiza valores de estado de distintivo en espera.
- Se ha añadido el nuevo umbral predefinido UDB_HADR_Aux_Standby_Disconnect para supervisar bases de datos en espera secundarias en un entorno HADR.
- Se actualiza el widget de uso de memoria de base de datos 5 principales para mostrar el valor correcto.
- El agente de Db2 da soporte ahora a las plataformas siguientes:
  - Ubuntu zLinux 18.04
  - SUSE Linux Enterprise Server 15 on x86-64 (64 bits)
  - SUSE Linux Enterprise Server 15 for zLinux
  - SUSE Linux Enterprise Server 15 for Power Linux Little Endian

Monitoring Agent for InfoSphere DataStage

El agente de InfoSphere DataStage se ha mejorado con las características siguientes:

- Se ha añadido la capacidad de inhabilitar la recopilación de datos para grupos de atributos seleccionados.
- Recopilación de datos optimizada para el grupo de atributos de ejecuciones de trabajos.
- Se ha añadido soporte para la plataforma SUSE Linux Enterprise Server 15.

Monitoring Agent for Internet Services

El agente de Internet Service Monitoring da soporte ahora a las plataformas Windows de 64 bits y Linux de 64 bits

Monitoring Agent for Microsoft .NET

El agente .NET se ha mejorado con las siguientes características:

- El agente .NET ahora realiza un seguimiento de las solicitudes fallidas. El estado de estas solicitudes se muestra como failed bajo el widget de grupo Solicitudes más recientes de la página Detalles de transacción de middleware. Además, el widget de grupo Errores más recientes lista las solicitudes fallidas más recientes junto con el código de estado y la descripción del error.
- El agente .NET también supervisa los datos de usuario a través de sesiones ASP.NET Identity y ASP.NET. Los datos de usuario se visualizan en el widget de grupo de 5 principales usuarios de la página Detalles de transacción de middleware.

Monitoring Agent for MongoDB

Agente de MongoDB da soporte ahora a la plataforma SUSE Linux Enterprise Server 15.

Monitoring Agent for NetApp Storage

El agente de NetApp Storage se ha mejorado con las siguientes características:

- Se ha añadido un nuevo recuadro de búsqueda en la página Detalles de sucesos que filtra los datos de sucesos basándose en los criterios de búsqueda.
- Se añade una nueva página Detalles para las LUN.
- El usuario puede ahora comprobar los detalles del dispositivo relacionado correlacionado con cada objeto de almacenamiento en la página **Detalles**.

Monitoring Agent for OpenStack

Se ha añadido soporte para supervisar instancias de máquina virtual, como el uso de la CPU de instancia de máquina virtual, memoria, disco y controlador de interfaz de red.

Monitoring Agent for PostgreSQL

- Se ha añadido soporte para SUSE Linux Enterprise Server 15
- Recopilación de datos optimizada para grupos de atributos de CPU y memoria

Monitoring Agent for RabbitMQ

Se ha añadido soporte para SUSE Linux Enterprise Server 15

Monitoring Agent for SAP Applications

El Agente de SAP ahora da soporte a las siguientes plataformas:

- Plataforma SUSE Linux Enterprise Server 15
- SAP NW RFC SDK 7.50

Monitoring Agent for Skype for Business Server

Skype for Business Server se ha mejorado con las siguientes características:

- Los mandatos de transacciones sintéticas en el módulo de transacciones sintéticas ahora son ejecutables por Usuarios de prueba ya configurados. Para hacer uso de esta característica, inhabilite `Utilizar valores de configuración de agente` en el panel Configuración de agente y proporcione un valor de `Nombre de dominio completo de agrupación` para el que se ejecutarán los mandatos sintéticos. Asegúrese de que el usuario de prueba se ha configurado a través del mandato NewCsHealthMonitoringConfiguration para la identidad proporcionada en el campo Nombre de dominio completo de agrupación del panel de configuración de agente.
- Los usuarios ahora pueden inhabilitar los mandatos sintéticos. Para inhabilitar cualquier mandato concreto de la ejecución, proporcione `false` en ese nombre de mandato en el archivo `LyncSyntheticTrans.exe.config` presente en la ubicación `<CANDLE_HOME>\tmaitm6` para la versión de 32 bits y `<CANDLE_HOME>\TMAITM6_x64` para la versión de 64 bits.

Monitoring Agent for Tomcat

- Se ha añadido un nuevo clúster de grupo de atributos. Contiene información de las propiedades de un clúster.
- Se ha añadido un nuevo widget de información de clúster. Este widget visualiza información del clúster de grupo de atributos. No se visualizará ningún dato si el agente está supervisando una configuración de Tomcat que no sea de clúster.
- Se ha añadido la variable del panel de configuración *Puerto de servidor Tomcat*. Esta variable representa el puerto en el que se está ejecutando el servidor Tomcat. El valor predeterminado de la variable es 8080.

Monitoring Agent for VMware VI

- La página Componente se ha mejorado para mostrar la dirección IP o el nombre de host de vCenter configurado y su conectividad con el agente.

Agente de WebSphere Infrastructure Manager

El agente de WebSphere Infrastructure Manager da soporte ahora a AIX.

Agente de WebSphere MQ

El agente de WebSphere MQ está ahora soportado en IBM WebSphere MQ 9.1.

Mejoras de recopiladores de datos

Recopilador de datos de J2SE

El Recopilador de datos de J2SE se ha mejorado con las características siguientes:

- Se ha añadido soporte para SUSE Linux Enterprise Server 11 for Power Linux Big Endian (64 bits).
- Se ha añadido soporte para Power Linux Big Endian (pLinux BE) (64 bits).
- Se ha añadido soporte para Power Linux Little Endian (pLinux LE) (64 bits).
- Se ha añadido supervisión del servidor Jetty y el módulo de configuración.

Soporte de plataforma ampliado para agentes

Ahora se da soporte a los siguientes agentes y plataformas:

Plataforma SUSE Linux Enterprise Server 15

- Agente de Cassandra
- Agente de DataPower

- Agente de DataStage
- Agente de Db2
- HTTP Server
- Agente de IBM Integration Bus
- Agente de sistema operativo Linux
- Agente de MongoDB
- Agente de OpenStack
- Agente de PostgreSQL
- Monitoring Agent for RabbitMQ
- Agente de SAP
- Agente de WebSphere MQ

Power Linux

- Recopilador de datos de J2SE

Ubuntu 18.04

- Agente de Cassandra
- Agente de IBM Integration Bus
- Agente de OpenStack
- Agente de sistema operativo Linux
- Agente de RabbitMQ
- Agente de WebSphere MQ

Soporte de Power 9

Ahora se da soporte a Power 9 para todos los agentes.

Novedades de la actualización de octubre de 2018 de V8.1.4

Integración con Cloud Event Management

Cloud Event Management proporciona gestión de incidencias en tiempo real entre los servicios, aplicaciones e infraestructura. Ahora, con la integración entre Cloud Event Management e IBM Cloud Application Performance Management, todos los sucesos generados en Cloud APM se envían a Cloud Event Management.

Septiembre de 2018

Nuevo agente disponible

Monitoring Agent for MQ Appliance

El agente de MQ Appliance proporciona información de supervisión que es específico para el nivel de dispositivo MQ en MQ Appliances, por ejemplo, información de memoria de CPU, memoria, almacenamiento, sensores y gestor de colas.

Mejoras en los agentes

Monitoring Agent for Db2

El agente de Db2 da soporte ahora al sistema operativo Power Linux Big Endian.

Monitoring Agent for Hadoop

- El agente Hadoop ahora supervisa el estado de dos servicios más: SmartSense y Druid.
- El agente Hadoop ahora da soporte a Hortonworks Data Platform (HDP) 3.0.0.

Agente de Internet Service MonitoringAgente

Se ha mejorado la funcionalidad de edición para el agente de Agente de Internet Service Monitoring. Todos los supervisores que tienen parámetros configurables se pueden editar.

Monitoring Agent for MySQL
El agente de MySQL ahora da soporte a la supervisión de MySQL v8.0.11.

Monitoring Agent for NetApp Storage
El agente de NetApp Storage se ha mejorado con las siguientes características:

- Se ha añadido un nuevo widget denominado Resumen de sucesos global en la página Instancia de almacenamiento de NetApp. Visualiza el recuento acumulativo de sucesos. Puede ver todos los sucesos que se han producido en el entorno, independientemente de la gravedad o del objeto pulsando la barra de estado representada como Sucesos totales.

  Además, se ha añadido una columna Estado de suceso en cada tabla de objetos, que muestra el estado de suceso priorizado basándose en el tiempo y, a continuación, el nivel de gravedad.

  La página Instancia de almacenamiento de NetApp ahora visualiza una tabla de resumen de sucesos en lugar de un gráfico.
- La página Datos agregados se actualiza para visualizar los dispositivos relacionados asociados con la suma seleccionada.

Monitoring Agent for SAP Applications
Soporte añadido para SAP NW RFC SDK 750.

Monitoring Agent for SAP HANA Database
Se han añadido dos nuevas características:

- La base de datos SAP HANA se puede supervisar en modo en espera.
- El Agente de SAP HANA Database da soporte a la plataforma Big Endian para Power System.

Monitoring Agent for VMware VI

- Ahora se da soporte a la supervisión de **HostVFlashManager**
- El panel de instrumentos del servidor ESX ahora muestra el recuento de máquinas virtuales que están en su estado Crítico, Aviso y Normal con respecto a la utilización de la CPU.

Nueva plataforma: Linux on POWER Big Endian
Hay una nueva plataforma disponible. Los siguientes agentes ahora están soportados en Linux on POWER Big Endian:

- Agente de Db2
- Agente de IBM Integration Bus
- Agente de sistema operativo Linux
- Agente de SAP HANA Database
- Agente de WebSphere MQ
- Agente de WebSphere Applications

Julio de 2018

Nuevos agentes disponibles

Monitoring Agent for Sybase Server

El Agente de Sybase ofrece un punto central de gestión de las bases de datos distribuidas. Recopila la información necesaria para que los administradores del sistema y de la base de datos puedan examinar el rendimiento del sistema del servidor Sybase, detectar problemas con antelación y evitarlos.

Mejoras en los agentes

Monitoring Agent for Hadoop

- Se ha añadido soporte para la supervisión de servicios de Hadoop como, por ejemplo, Mahout, Atlas y Falcon.
- Se ha añadido soporte para la supervisión de la oferta de Hadoop: Cloudera CDH 5.13.

- Se ha añadido soporte para la supervisión de la oferta de Hadoop: Hortonworks HDP 2.6.4.

Monitoring Agent for HMC Base

Ahora se ha soporte a HMC V8 R8.7.0.

Monitoring Agent for HTTP Server

Se ha añadido soporte para Apache HTTP Server de 64 bits en Windows.

Monitoring Agent for Microsoft .NET

Se ha mejorado el Monitoring Agent for Microsoft .NET de la forma siguiente:

- El módulo Tiempo de respuesta de IIS ahora supervisa la subtransacción y representa el desglose de tiempo mediante inyección JavaScript para formularios web ASP.NET (páginas .aspx) y vistas de ASP.NET MVC, que cumplen las condiciones siguientes:
  - La página cumple los estándares W3C HTML.
  - Las cabeceras de respuesta contienen `Content-Type: text/html, application/xml,application/json`.
  - El contenido de respuesta incluye el elemento *<head>*.
- El agente .NET carga los datos de búsqueda en profundidad en el servicio Diagnostic Query Engine (DQE) en el servidor APM. El panel de instrumentos de búsqueda en profundidad del servicio DQE carga y muestra rápidamente los datos.
- Se ha añadido el nuevo umbral **`NET_Slow_IIS_Request_Crit`** que se desencadena cuando el widget 10 más lentas tiene solicitudes con tiempos de respuesta superiores a 500 milisegundos.
- La herramienta de filtrado selectivo se ha actualizado con un recuadro de búsqueda para la búsqueda de una agrupación de aplicaciones desde la lista de agrupaciones de aplicaciones.
- Se ha añadido el programa de utilidad **`ProcListCaller`** para proporcionar la lista de procesos que han cargado el perfilador CLR de .NET (`CorProfLog.dll`).

Monitoring Agent for Microsoft SQL Server

- Ahora el Agente de Microsoft SQL Server da soporte a varias ordenaciones en el análisis de ERRORLOG según los valores de ordenación establecidos en el archivo `koqErrConfig.ini`. Si el archivo `koqErrConfig.ini` no contiene valores de ordenación válidos, sólo podrá ver el mensaje de error predeterminado en inglés con un nivel de gravedad superior al nivel de gravedad predeterminado, si lo hay. El nivel de gravedad predeterminado es 17. Al analizar el archivo ERRORLOG, se considerarán todas las ordenaciones existentes en el archivo `koqErrConfig.ini`. Por lo tanto, sólo se deben añadir al archivo `koqErrConfig.ini` las ordenaciones que están en uso. El análisis de ERRORLOG distingue entre mayúsculas y minúsculas, debe asegurarse de que los valores de palabra clave de ordenación en el archivo `koqErrConfig.ini` son exactamente los mismos que los valores de palabra clave que se encuentran en el archivo ERRORLOG o en el archivo `koqErrConfigSample.ini` de referencia. Tenga en cuenta que los cambios realizados en el archivo `koqErrConfig.ini` no se conservan durante la actualización del agente. Debe hacer una copia de seguridad antes de actualizar el agente.
- El agente también proporciona la herramienta de programa de utilidad **`koqVerifyPermissions.exe`** para comprobar si un usuario existente de SQL Server tiene permisos suficientes para supervisar Microsoft SQL Server. Si un usuario existente de SQL Server no tiene permisos suficientes, puede utilizar la herramienta de programa de utilidad **`permissions.cmd`** como alternativa para otorgar los permisos mínimos a un usuario existente de SQL Server para la recopilación de datos.

Monitoring Agent for NetApp Storage

Se ha mejorado el Monitoring Agent for NetApp Storage de la forma siguiente:

- Se ha añadido la nueva página Componente para mostrar los detalles de estado de conexión del agente de si el proveedor de datos está activo o inactivo, junto con la dirección IP de los

orígenes de datos supervisados. La barra de estado individual representa el número de nodos, agregados, volúmenes y discos que están en estado crítico, normal, de aviso o desconocido.

- Se ha añadido la nueva página Instancia de almacenamiento de NetApp para resaltar las propiedades principales de los clústeres, agregados, volúmenes, discos y vServers. También muestra el gráfico Resumen de sucesos con el recuento de sucesos correspondientes a cada entidad u objeto de almacenamiento disponible en el entorno. Por ejemplo, si hay 12 volúmenes configurados y cada volumen tiene dos sucesos con una gravedad Crítica, el gráfico Resumen de sucesos muestra el recuento total de sucesos que se han producido en todos los volúmenes disponibles en un entorno. En este caso, el gráfico muestra una barra con 24 sucesos críticos en el volumen como una entidad trazada en el eje X.
- Se ha actualizado la página Detalles de nodo para mostrar los detalles de los puertos de la red.
- Se ha actualizado la página Detalle de volumen para mostrar los detalles de las duplicaciones de instantáneas asociados y el recuento de LUN de cada volumen seleccionado.
- Se ha actualizado la página Detalles de vServers para mostrar la información sobre las interfaces lógicas de red.

Monitoring Agent for Tomcat
Ahora el servidor Tomcat V9.0.5 está soportado.

Monitoring Agent for WebSphere MQ

La supervisión remota está soportada. Se han añadido dos parámetros de configuración para que el agente pueda recopilar datos de supervisión para el gestor de colas remoto. No obstante, estos parámetros de configuración no tienen ningún efecto sobre un gestor de colas local. Si desea configurar el agente para supervisar un gestor de colas local, puede pulsar Intro para omitir la especificación de estos parámetros.

Para obtener más información sobre la configuración del agente, consulte "Configuración del Agente de WebSphere MQ" en la página 968.

Mejora de la personalización de los atributos EIF

Ahora puede añadir varios valores de atributo y valores literales al atributo EIF. Por ejemplo, en lugar de un mensaje `El porcentaje de disco libre es` **`Disk_Free_Percent`** para un umbral que comprueba si queda poco espacio de disco libre, podría tener `El porcentaje de disco libre es` **`Disk_Free_Percent`** `y el porcentaje de inodos libres es` **`Inodes_Free_Percent`**. El mensaje reenviado podría ser similar al siguiente: `El porcentaje de disco libre es 13 y el porcentaje de inodos libres es 9`. Para obtener más información, consulte "Personalización de un suceso para reenviarlo a un receptor EIF" en la página 1025.

Abril de 2018

Nuevo agente disponible

Monitoring Agent for AWS Elastic Load Balancer

El Agente de Amazon ELB proporciona un punto central de supervisión del estado, la disponibilidad y el rendimiento de los Equilibradores de carga elásticos de AWS. El agente muestra un conjunto exhaustivo de métricas para cada aplicación de tipo equilibrador de carga, ayuda de red y clásica para ayudarle a tomar decisiones sobre su entorno de Equilibrador de carga elástico de AWS basadas en información.

Mejoras en los agentes

Agente de Supervisión de tiempo de respuesta
El Módulo de Tiempo de respuesta de IBM HTTP Server da soporte ahora a IBM HTTP Server versión 7, 8 y 9 en Windows.

Monitoring Agent for Node.js
De forma predeterminada, Recopilador de datos de Node.js ya no recopila la información confidencial de usuario como por ejemplo cookies, contextos de solicitud HTTP y contextos de

solicitud de base de datos. Puede cambiar este comportamiento predeterminado especificando la variable de entorno nueva *SECURITY_OFF*.

Monitoring Agent for Amazon EC2
El nombre de componente refleja ahora el nombre de agente.

Se ha añadido soporte ampliado de retención de datos.

Monitoring Agent for WebLogic
El rastreo de transacciones y el diagnóstico en profundidad están habilitados en AIX. Anteriormente, estas características solo estaban habilitadas en Linux y Windows.

Se ha mejorado el Resumen de solicitud detallado para servlets implementados con anotaciones para el rastreo de transacciones y el diagnóstico en profundidad.

Monitoring Agent for Skype for Business Server
Soporte para Windows Server 2016.

Monitoring Agent for Sterling File Gateway
El agente capta sucesos para transferencias de archivos anómalas como comportamiento predeterminado. Puede cambiar este comportamiento especificando el valor adecuado de la variable de entorno nueva **KFG_ALL_FGEVENTS**.

Monitoring Agent for Sterling Connect Direct
Se ha mejorado la característica de registro de agente. Para obtener más información, consulte la sección Resolución de problemas.

Mejoras de recopiladores de datos

Recopilador de datos de Node.js
De forma predeterminada, Recopilador de datos de Node.js ya no recopila la información confidencial de usuario como por ejemplo cookies, contextos de solicitud HTTP y contextos de solicitud de base de datos. Puede cambiar este comportamiento predeterminado especificando la variable de entorno nueva *SECURITY_OFF*.

Recuerde: Para obtener esta mejora, debe descargar y aplicar el arreglo temporal 1 de IBM Cloud Application Performance Management Recopilador de datos de Node.js de IBM Fix Central. Para obtener más información, consulte el archivo léame del arreglo temporal 1.

Recopilador de datos de J2SE
Se ha añadido soporte para el descubrimiento automático de la clase de punto de entrada (clase main) y el nombre de alias de la aplicación J2SE.

El rastreo de transacciones y el diagnóstico en profundidad se pueden habilitar e inhabilitar localmente mediante scripts de configuración.

Mejoras en la documentación
Se ha creado una página web en Application Performance Management Developer Center para ayudarle a encontrar el nivel de agente en cada actualización o release. Para obtener más información, consulte Agent version in Cloud APM releases.

Las prestaciones de agente y recopilador de datos en cada tabla de oferta se han simplificado para mejorar su lectura. Para obtener más información, consulte “Capacidades” en la página 54.

Febrero de 2018

Nuevo agente disponible

Monitoring Agent for Azure Compute

El Agente de Azure Compute proporciona un punto central de supervisión del estado, la disponibilidad y el rendimiento de las instancias de Azure Compute. El agente muestra un conjunto de métricas integral para ayudarle a tomar decisiones informadas sobre el entorno de Azure Compute. Estas métricas incluyen el uso de CPU, el uso de red y el rendimiento de disco.

Monitoring Agent for Sterling Connect Direct

Puede utilizar el Agente de Sterling Connect Direct para supervisar el estado y el rendimiento del servidor de Sterling Connect Direct. Supervisa las funciones del servidor de Sterling Connect Direct como, por ejemplo, las actividades de transferencia de archivos, los procesos planificados y los procesos de retención y espera en cola. El agente admite la supervisión remota y es para múltiples instancias.

Monitoring Agent for Sterling File Gateway

El Agente de Sterling File Gateway supervisa la aplicación Sterling File Gateway, que se utiliza para transferir archivos entre socios internos y externos utilizando diferentes protocolos, diferentes convenciones de nomenclatura y diferentes formatos de archivo. También admite la función de supervisión remota.

Mejoras en los agentes

Monitoring Agent for DataPower
Se da soporte al rastreo de transacciones entre el Agente de WebSphere MQ y el Agente de DataPower .

Monitoring Agent for Db2
Se ha añadido soporte para la supervisión remota.

Monitoring Agent for Hadoop
Se ha añadido soporte para la supervisión del estado de dispositivos Hadoop como, por ejemplo, HBase, MapReduce2, Tez y Ranger.

Se ha añadido soporte para la supervisión de la oferta de Hadoop: Cloudera CDH 5.12.

Monitoring Agent for InfoSphere DataStage
Se ha añadido soporte para MS SQL como repositorio de metadatos.

Se ha añadido soporte para el sistema operativo Windows.

Monitoring Agent for Tomcat
Soporte al rastreo de transacciones y al diagnóstico en profundidad para PLinux mediante la actualización de la infraestructura de agente con el parche 8.1.4.0-IBM-APM-SERVER-IF0001.

Monitoring Agent for SAP Applications
Mejora para la función CCMS: automatización de la detección de archivos `idx`. Esta automatización solamente funciona cuando se reinicia el sistema SAP.

Monitoring Agent for Microsoft .NET
Se ha añadido soporte para las transacciones de usuario final utilizando el módulo Tiempo de respuesta de IIS.

Monitoring Agent for Skype for Business Server
El nombre del agente cambia de Monitoring Agent for Microsoft Lync Server a Monitoring Agent for Skype for Business Server.

Monitoring Agent for Linux KVM
Se ha añadido soporte para RHEV-M 4.x.

Monitoring Agent for Linux OS
Se ha modificado el intervalo de carga de memoria a 1 minuto.

Se visualiza la dirección IP asociada a la interfaz de red en el panel de instrumentos del sistema operativo Linux y el widget Información del sistema.

Monitoring Agent for UNIX OS
Se ha modificado el intervalo de carga de memoria a 1 minuto.

Mejoras de recopiladores de datos

Recopilador de datos de J2SE
Se ha añadido soporte para Spring Boot Applications.

Mejoras del Availability Monitoring

Con el complemento Availability Monitoring, puede crear listas blancas y listas negras para especificar los URL que a los que pueden y no pueden acceder las pruebas. La lista blanca y la lista negra controlan las dependencia y los recursos que contribuyen a los tiempos de respuesta de las aplicaciones web probadas como, por ejemplo, medidas de terceros. Filtre los URL por esquema, dominio o tipo de archivo utilizando los caracteres comodín.

Diciembre de 2017

Nuevo agente disponible

Monitoring Agent for InfoSphere DataStage

Puede utilizar el Agente de DataStage para supervisar el estado y el rendimiento de los recursos de servidor de DataStage, como por ejemplo los servicios de motor, sistemas de motor, actividad de trabajos, estados de ejecución de trabajos y detalles de las ejecuciones de trabajos. Este agente admite la supervisión remota.

Mejoras en los agentes

Monitoring Agent for Hadoop

Se ha añadido soporte para supervisar un clúster Hadoop protegido con la autenticación basada en Kerberos SPNEGO, que utiliza el KDC (centro de distribución de claves) de Active Directory.

Se ha añadido soporte para probar la conexión a hosts de un clúster Hadoop que está protegido con autenticación basada en Kerberos SPNEGO, que utiliza MIT o Active Directory como KDC (centro de distribución de claves).

Se ha añadido soporte para supervisar las siguientes ofertas de Hadoop: Cloudera CDH 5.10 y CDH 5.11.

Se ha añadido soporte para supervisar el estado de los servicios de Hadoop, como Flume, Kafka, Titan, Spark, Knox, Pig, Slider y Solr.

Monitoring Agent for HTTP Server

Se ha añadido soporte para IBM HTTP Server y Apache HTTP Server Windows de 32 bits.

Se ha añadido soporte para Linux for System z (El rastreo de transacciones no está soportado).

Se ha añadido soporte para el servidor HTTP de Oracle en Linux for System x.

Monitoring Agent for IBM Integration Bus

Se ha añadido soporte para Linux for Power Systems (Little Endian).

Monitoring Agent for Microsoft .NET

Se ha añadido soporte para ODP.NET.

Se han añadido detalles de rastreo de método para el método HttpWebRequest.GetResponse().

Monitoring Agent for Microsoft SQL Server

Se ha añadido soporte de tolerancia para SQL Server 2017.

Se ha añadido soporte para la característica Always On para la edición de desarrolladores de SQL Server.

Monitoring Agent for MySQL

Se ha añadido soporte de tolerancia para las tablas de esquema de información que se migran al esquema de rendimiento.

Se ha añadido soporte para tablas en desuso de esquema de información mediante el esquema de rendimiento.

Monitoring Agent for Microsoft Internet Information Services

Se ha añadido soporte para la supervisión de sitios web de FTP.

Monitoring Agent for MongoDB

Se ha añadido soporte para la supervisión remota.

Se ha añadido soporte para la supervisión del motor de almacenamiento en memoria.

Monitoring Agent for OpenStack
Se ha añadido soporte para la API de autenticación de OpenStack V3.

Monitoring Agent for Oracle Database
La versión de agente se ha cambiado a 8.0.

Se ha añadido el parámetro de configuración **Archivo jar JDBC de Oracle** y los parámetros de configuración **Directorio de inicio de Oracle** y **Directorio de instalación del cliente de Oracle Instant** se han eliminado.

Monitoring Agent for PostgreSQL
Se ha añadido soporte para la supervisión remota.

Monitoring Agent for SAP Applications
Se ha añadido soporte para la comunicación SNC.

Se ha añadido un nuevo umbral para el sistema SAP inactivo.

Monitoring Agent for SAP NetWeaver Java Stack
Se ha añadido la posibilidad de restaurar la instancia de SAP NetWeaver Application Server.

Monitoring Agent for Tomcat
Se ha añadido soporte para Linux for Power Systems (Little Endian) (sólo supervisión de recursos).

Monitoring Agent for VMware VI
Se han añadido Resumen de red y Recuento de disco en la página de visión general de ESX Server.

Se ha añadido el widget de grupo de sucesos a la página de resumen de clúster.

Monitoring Agent for WebSphere Applications
Se ha añadido soporte de rastreo de transacciones para Linux for Power Systems (Little Endian) y para Linux for System z.

Recuerde: Para obtener el soporte de rastreo de transacciones en Linux for Power Systems (Little Endian) y Linux for System z, siga estos pasos:

1. Descargue la imagen de instalación del agente.
2. Instale la Agente de WebSphere Applications.
3. Descargue el arreglo temporal 2 del Agente de WebSphere Applications de Fix Central.
4. Siga el archivo léame del arreglo temporal para aplicar el arreglo.

Monitoring Agent for WebSphere MQ
Se ha añadido el widget de grupo Estado de servicio de MQ para proporcionar detalles del servicio MQ.

Se ha añadido soporte para Linux for Power Systems (Little Endian).

Mejoras de recopiladores de datos

Recopilador de datos de Liberty
El nombre de sistema gestionado (MSN) registrado por el Recopilador de datos de Liberty se ha cambiado para reflejar el nombre de host y el nombre del servidor de Liberty. El nuevo MSN para este recopilador de datos es `BI:`*`nombreservidor_nombrehost_md5`*`:`BLP, donde *md5* es el GUID de la aplicación local basado en MD5. La longitud de *nombreservidor_nombrehost_md5* es de 25 caracteres.

Recuerde: Para obtener esta mejora, debe descargar y aplicar el arreglo temporal 1 del recopilador de datos de Liberty de IBM Cloud Application Performance Management de Fix Central.

Recopilador de datos de J2SE
Se ha añadido soporte de rastreo de transacciones para aplicaciones J2SE.

Mejoras en la documentación

Se proporciona la información sobre los puertos predeterminados utilizados por los agentes y recopiladores de datos para facilitar la preparación del entorno. Consulte "Puertos predeterminados utilizados por los agentes y recopiladores de datos" en la página 87.

Se proporciona la información sobre nombres de sistema gestionado (MSN) de agentes de Cloud APM. También se proporcionan instrucciones sobre cómo cambiar la serie de nombre de host del MSN. Consulte "Nombres de sistema gestionado" en la página 173.

se proporciona la información sobre la ejecución del agente como un usuario no administrador o los permisos que son necesarios para ejecutar el agente con usuario no administrador en los temas de configuración para los agentes siguientes:

- Agente de Microsoft .NET
- Agente de Microsoft Active Directory
- Agente de Microsoft Exchange Server
- Agente de Skype for Business Server
- Agente de Microsoft SharePoint Server
- Agente de Microsoft SQL Server
- Agente de Tomcat

Agosto de 2017

IBM Cloud Application Performance Management, Availability Monitoring

El complemento Availability Monitoring proporciona una supervisión sintética mejorada de las aplicaciones web desde varios puntos de presencia alrededor del mundo. Cree pruebas sintéticas que simulan el comportamiento del usuario a intervalos regulares. Ejecute sus pruebas desde puntos de presencia públicos o descargue y despliegue sus propios puntos de presencia en servidores locales o privados. Utilice el panel de instrumentos Availability Monitoring para supervisar la disponibilidad, el rendimiento y las alertas de la aplicación mediante gráficos, tablas de desglose y vistas de mapa. Utilice el análisis en cascada para identificar cuándo se producen problemas de rendimiento y disponibilidad y averiguar las razones de esos problemas.

Supervisión de IBM API Connect

Los agentes y recopiladores de datos de Cloud APM dan soporte ahora a la supervisión del entorno IBM API Connect. Puede desplegar los agentes y recopiladores de datos correspondientes para obtener visibilidad del estado y el rendimiento de los componentes del entorno. Además de la supervisión de recursos y los datos de diagnóstico detallado, también están disponibles los datos de rastreo de transacciones, lo que permite ver información de topología sobre el entorno IBM API Connect. Para obtener más información, consulte "Escenario: Supervisión de IBM API Connect" en la página 92.

Soporte de sistema operativo

Linux for System z

Se ha añadido soporte de Linux for System z para los agentes de supervisión siguientes: Linux OS, WebSphere Application, Db2, WebSphere MQ, IBM Integration Bus, Tomcat y Response Time Monitoring.

Linux for Power Systems (Little Endian)

Se ha añadido soporte Linux para Power Systems (Little Endian) para los siguientes agentes de supervisión: Linux OS, WebSphere Application y Db2.

Linux for System x

Se ha añadido Linux on System x para dar soporte al recopilador de datos de Liberty.

Soporte del agente de SO IBM i

Los datos del agente SO IBM i se pueden ahora visualizar en Consola de Cloud APM. Este agente es un agente de IBM Tivoli Monitoring V6 y permanece como un agente de V6 para el release V8.1.4. Puede utilizar Pasarela híbrida para recuperar los datos del agente y enviarlos al Servidor de Cloud APM. Como resultado, puede visualizar los sucesos y datos de supervisión para este agente en la Consola

de Cloud APM. Para obtener más información sobre el agente SO IBM i, consulte los Agentes soportados por la pasarela híbrida (APM Developer Center).

Nuevos agentes disponibles

Monitoring Agent for OpenStack

Puede utilizar el Agente de OpenStack para supervisar el estado y el rendimiento de las aplicaciones OpenStack y ver información como por ejemplo la información sobre puntos finales de API, conexión de servidor SSH, procesos e hipervisores.

Hay recopiladores de datos nuevos y mejorados disponibles

Puede utilizar los recopiladores de datos para supervisar el estado y el rendimiento de las aplicaciones siguientes en IBM Cloud, en local o en ambos casos:

Recopilador de datos de J2SE

Puede utilizar el Recopilador de datos de J2SE para supervisar el estado y el rendimiento de las aplicaciones Java y ver datos de diagnóstico, como por ejemplo tiempo de respuesta, rendimiento, contexto de solicitudes y rastreo de método de solicitudes.

Recopilador de datos de Liberty

El Recopilador de datos de Liberty supervisa el perfil de Liberty en el entorno de IBM Cloud y el perfil de Liberty local en Linux for System x.

Recopilador de datos de Node.js

El Recopilador de datos de Node.js supervisa aplicaciones locales y de IBM Cloud. Puede ver datos de supervisión de recursos y de diagnóstico, como por ejemplo la utilización de recursos, el rendimiento e información detallada acerca de solicitudes y métodos.

Recopilador de datos de Python

El Recopilador de datos de Python supervisa aplicaciones de IBM Cloud. Puede ver datos de supervisión de recursos y de diagnóstico, como por ejemplo la utilización de recursos, el rendimiento e información detallada acerca de solicitudes y métodos.

El Agente de Python se ha eliminado del paquete de instalación de agente en Cloud APM V8.1.4. Solo puede utilizar el Recopilador de datos de Python para supervisar las aplicaciones Python.

Recopilador de datos de Ruby

El Recopilador de datos de Ruby supervisa solo aplicaciones IBM Cloud. Puede ver datos de supervisión de recursos y de diagnóstico, como por ejemplo la utilización de recursos, el rendimiento e información detallada acerca de solicitudes y métodos.

Mejoras en los agentes

Monitoring Agent for Amazon EC2

- El agente puede manejar correctamente fechas finales nulas para los sucesos planificados.
- Se ha añadido soporte para un proxy de reenvío entre el agente Amazon EC2 y Amazon Web Services

Monitoring Agent for Citrix Virtual Desktop Infrastructure

- Se ha añadido la supervisión de sucesos de Windows y medidas de PowerShell incluso cuando el agente está instalado en un sistema Linux
- Se ha añadido la página **Sesiones de VDA**, a la que puede acceder a través de la página**Detalles de máquina VDA**.
- Se ha añadido el widget Métricas de máquina a la página **Detalles de máquina VDA**.
- Se ha mejorado la configuración Controlador de entrega de escritorio (DDC) para habilitar el agente para que maneje la migración tras error DDC en un entorno distribuido.

Monitoring Agent for Db2

- Se ha añadido soporte para Linux for System z.

Monitoring Agent for Hadoop

- Se ha añadido soporte para supervisar las ofertas de Hadoop siguientes: Hortonworks HDP 2.6 y Cloudera CDH 5.9, 5.10 y 5.11
- Se ha añadido soporte para supervisar el estado de servicios de Hadoop como por ejemplo ZooKeeper, Sqoop, Hive, HDFS, YARN, Ambari Metrics y Oozie.
- Se ha añadido soporte para supervisar un clúster Hadoop protegido con la autenticación basada en Kerberos SPNEGO, que utiliza solo MIT Kerberos V5 Key Distribution Center (KDC).

Monitoring Agent for IBM Integration Bus

Se ha añadido soporte para Linux for System z (El rastreo de transacciones no está soportado).

Monitoring Agent for JBoss

- El proceso de configuración de diagnóstico detallado y rastreo de transacciones se ha simplificado para el agente de JBoss en la oferta Advanced Agents.
- Se han añadido dos widgets de panel de instrumentos a la página **Detalles de recogida de basura**. Un widget muestra la cantidad de memoria de almacenamiento dinámico que se ha liberado desde la última recogida de basura y el otro widget muestra los tamaños de agrupación de memoria de almacenamiento dinámico edén/superviviente/permanente (generación antigua) históricos.

Monitoring Agent for Linux OS

Se ha añadido soporte para Linux for Power Systems (Little Endian).

Monitoring Agent for Skype for Business Server

- Se ha añadido el widget de grupo Resumen de uso de Lync al el panel de instrumentos Visión general de servidor Lync para ver el estado de registro frontal y la calidad baja de llamadas.
- Se ha añadido un panel de instrumentos nuevo para visualizar los detalles del uso de Microsoft Lync Server.

Monitoring Agent for SAP NetWeaver Java Stack

Se han añadido las mejoras siguientes al panel de instrumentos del Agente de SAP NetWeaver Java Stack:

- Se han añadido conjuntos de datos, widgets de grupo y páginas para recopilar y ver los datos de diagnóstico y rastreo de transacciones.
- Se ha añadido soporte para instalar y configurar el agente en sistemas Windows 2016.
- Se ha añadido el widget de grupo 5 principales solicitudes más lentas por tiempo de respuesta al panel de instrumentos Instancia Java de SAP NW para proporcionar información sobre las 5 principales solicitudes realizadas por el usuario en la aplicación con el tiempo de respuesta más alto.
- La información de diagnóstico sobre las solicitudes visualizadas en el widget de grupo 5 principales solicitudes más lentas por tiempo de respuesta se puede ver en la página Instancias de solicitud pulsando la Solicitud. Se ha añadido soporte para visualizar la información de diagnóstico sobre las solicitudes en el widget de grupo 5 principales solicitudes más lentas por tiempo de respuesta.
- Se ha eliminado el widget de grupo 5 principales solicitudes más lentas por tiempo de respuesta.

Monitoring Agent for MongoDB

Se ha añadido soporte para supervisar el clúster de MongoDB o la configuración de réplica cuando el nodo primario falla.

Monitoring Agent for MySQL

Se han añadido conjuntos de datos y un parámetro de configuración para supervisar remotamente recursos de MySQL.

Monitoring Agent for NetApp Storage

- Se ha actualizado la página Componente para mostrar la información resumida de clústeres y Vservers.
- Se ha actualizado la página Instancia de almacenamiento de NetApp para mostrar información sobre los clústeres.

Monitoring Agent for Node.js

Se han añadido las mejoras siguientes al Agente de Node.js para utilizar Métricas de aplicación de nodo (Appmetrics):

- Nuevos widgets de grupo y de panel de instrumentos para ver detalles de recogida de basura.
- Nuevos widgets de grupo y de panel de instrumentos para ver detalles de bucle de sucesos

Monitoring Agent for PostgreSQL

- Soporte para instalar y configurar el agente en sistemas Windows.
- Soporte para supervisar PostgreSQL V9.6.
- Se ha actualizado la página **Visión general de estado** de modo que el estado no sea crítico cuando el índice de coincidencias del almacenamiento intermedio sea cero.

Monitoring Agent for SAP HANA Database

Se han añadido el atributo Días para caducidad de licencia y los umbrales HANA_License_Expiry_Crit_SYS y HANA_License_Expiry_Warn_SYS para supervisar el número de días que quedan hasta que la licencia caduque.

Monitoring Agent for Tomcat

- Se ha añadido soporte para Linux for System z
- Se han añadido conjuntos de datos, paneles de instrumentos y widgets de grupo para el rastreo de transacciones y el diagnóstico detallado.

Monitoring Agent for VMware VI

Se ha actualizado el widget de grupo Servidor ESX en el panel de instrumentos Resumen del servidor para mostrar el estado de SSH.

Monitoring Agent for WebLogic

El rastreo de transacciones y el diagnóstico detallado se han añadido al agente en la oferta Advanced Agents.

Monitoring Agent for WebSphere Applications

Se ha añadido soporte para Linux for System z (El rastreo de transacciones no está soportado).

Monitoring Agent for WebSphere MQ

Se ha añadido soporte para Linux for System z (El rastreo de transacciones no está soportado).

Se da soporte a los datos de historial a largo plazo de canal y de cola. Una vez que el gestor de colas está configurado para recopilar datos de estadísticas de canal o de cola, puede configurar el agente para habilitar la recopilación de datos de historial de canal o de cola a largo plazo. Aunque no hay paneles de instrumentos o widgets predefinidos para visualizar los datos de historial a largo plazo recogidos, puede utilizar la pestaña **Detalles de atributo** para consultar los datos recopilados en las tablas personalizadas.

Agente de Supervisión de tiempo de respuesta

- Se ha añadido soporte para IBM HTTP Server y Apache HTTP Server Windows de 32 bits.
- Se ha añadido soporte para configurar el seguimiento de usuarios para aplicaciones a la página **Configuración de agente**.
- Se ha añadido soporte para configurar el seguimiento de sesiones para aplicaciones a la página **Configuración de agente**.

Visualización mejorada

Vistas personalizadas

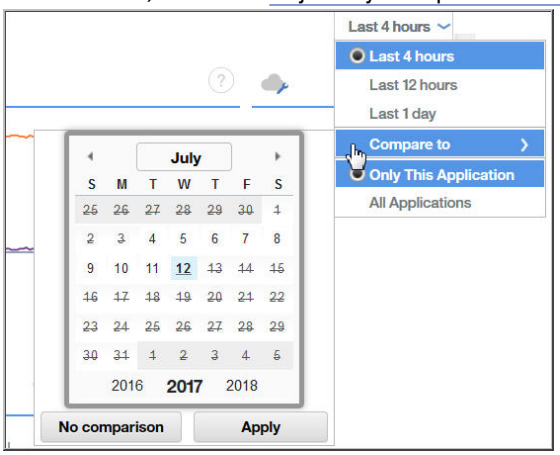
Puede utilizar IBM Cloud Application Business Insights Universal View para crear páginas personalizadas para las aplicaciones que está supervisando. En la pestaña Vistas personalizadas puede utilizar una plantilla existente o crear plantillas personalizadas para la página. Puede elegir entre las diferentes opciones de gráfico y métrica para crear widgets para supervisar datos según sus necesidades.

Al utilizar Universal View, puede crear paneles de instrumentos para supervisar datos de varios agentes. Puede exportar los datos de página personalizados a un archivo de datos en bruto.

Para obtener más información, consulte "Vistas personalizadas" en la página 1147.

Calendario para comparar los datos de un día anterior

Cuando está viendo gráficos de líneas que muestran datos históricos, se abre un calendario al elegir la opción de selector de tiempo para comparar el periodo de tiempo de un día anterior. Los días que no están disponibles para la comparación aparecen tachados. Para obtener más información, consulte "Ajuste y comparación de métricas a lo largo del tiempo" en la página 1125.



Mejoras en Agent Builder

Cuando crea un agente para supervisar datos desde una base de datos de Java Database Connectivity (JDBC), puede modificar los valores de enumeración establecidos para error, datos que faltan y ningún valor para evitar que se solapen con valores legítimos de la base de datos.

Puede establecer la Autoridad de indicación de fecha y hora para archivos JAR en la ventana **Preferencias** de Agent Builder. El el certificado de firma de Autoridad de indicación de fecha y hora caduca, puede establecer una autoridad nueva para seguir verificando archivos JAR.

Integración mejorada

Atributos de EIF personalizables para sucesos

Cuando el reenvío de sucesos está configurado, puede personalizar el mensaje de atributo EIF base y crear atributos EIF personalizados para sucesos enviados a un receptor, como por ejemplo Netcool/OMNIbus. El Editor de umbrales tiene un campo **¿Reenviar suceso EIF?** y un botón **Personalización de atributo EIF** para personalizar cómo se correlacionan los sucesos con sucesos reenviados. Para obtener más información, consulte "Personalización de un suceso para reenviarlo a un receptor EIF" en la página 1025.

Varias Pasarelas híbridas

En releases anteriores podía instalar Pasarela híbrida en un solo dominio de IBM Tivoli Monitoring que tiene un hub Tivoli Enterprise Monitoring Server. Ahora puede instalar Pasarela híbrida en varios dominios de Tivoli Monitoring. La categoría Pasarela híbrida de la página **Configuración avanzada** de la Consola de Cloud APM se ha trasladado a su propia página **Hybrid Gateway Manager**. Aquí puede crear y editar perfiles de Pasarela híbrida para supervisar sistemas gestionados desde varios dominios de Tivoli Monitoring, un perfil para cada dominio. Para obtener más información, consulte "Pasarela híbrida" en la página 987.

Escalabilidad mejorada

El número máximo de sistemas gestionados que puede supervisar desde Cloud APM ha aumentado de 4.000 a 10.000.

Releases anteriores

Para obtener información sobre nuevas características, prestaciones y cobertura en los releases anteriores, consulte los temas *Novedades* siguientes:

- "Novedades: abril de 2017" en la página 28
- "Novedades: septiembre de 2016" en la página 35
- Novedades: abril de 2016

Novedades: abril de 2017

Hay características, prestaciones y cobertura nuevas disponibles en el release de abril de 2017 de Cloud APM.

Nuevo Application Performance Management Developer Center

APM Developer Center es una ubicación central desde la que puede acceder a recursos para los productos APM: blogs, vídeos, documentación, soporte, sucesos, IBM Marketplace, etc. El menú **Ayuda** de la Consola de Cloud APM contiene un enlace a Application Performance Management Developer Center.

Rediseño de marca y simplificación del producto

IBM Performance Management on Cloud se denomina ahora IBM Cloud Application Performance Management. Los nombres de los componentes también han cambiado. Por ejemplo, la Consola de Cloud APM y el Servidor de Cloud APM se denominaban consola de Performance Management y servidor de Performance Management en releases anteriores.

Las ofertas de suscripción de IBM Performance Management on Cloud se han consolidado y renombrado:

Nombre de la oferta en el release de Octubre de 2016 y anteriores	Nombre de la oferta en el release de Marzo de 2017 y posteriores
Monitoring on Cloud	Cloud APM, Base
Application Performance Management Advanced on Cloud	Cloud APM, Advanced

Algunas extensiones de producto se han consolidado y renombrado:

Nombre de la extensión en el release de Octubre de 2016 y anteriores	Nombre de la extensión en el release de Marzo de 2017 y posteriores
Base Extension Pack (Agente de Hadoop)	Base Extension Pack (añade el nuevo Agente de Cassandra y el Agente de Microsoft Office 365)
Advanced Extension Pack (Agente de SAP HANA Database y Agente de SAP NetWeaver Java Stack)	Advanced Extension Pack (añade el nuevo Agente de RabbitMQ)

Soporte de sistema operativo

Sistemas operativos Windows 2016

Se ha añadido soporte para sistemas operativos Windows 2016. Para obtener más información, consulte el informe de compatibilidad de productos de software (SPCR) para todos los agentes: http://ibm.biz/agents-pm-systemreqs

Busque su sistema operativo en la sección Windows del informe y pulse el icono del componente para obtener una lista de los agentes soportados.

Nuevo paquete de ampliación disponible

IBM Cloud Application Performance Management z Systems Extension Pack

z Systems Extension Pack habilita el soporte para los agentes de IBM OMEGAMON en la oferta de Cloud APM. Los datos de agente de OMEGAMON se envían al Servidor de Cloud APM mediante la Pasarela híbrida. La Pasarela híbrida recupera los sucesos y datos de agente de OMEGAMON de la infraestructura de IBM Tivoli Monitoring a la que están conectados los agentes de OMEGAMON. Como resultado, puede ver los datos y sucesos de supervisión para los agentes de OMEGAMON en la Consola de Cloud APM.

Cloud APM z Systems Extension Pack está disponible en cualquiera de las ofertas de Cloud APM.

Para integrar este paquete de ampliación con Cloud APM, siga los pasos de la sección "Integración con OMEGAMON" en la página 999.

Nuevos agentes y recopiladores de datos disponibles

Monitoring Agent for Cassandra

Puede utilizar el Agente de Cassandra para supervisar el estado y el rendimiento de los recursos de clúster de Cassandra, como por ejemplo los nodos, espacios de claves y familias de columnas.

Monitoring Agent for Microsoft Office 365

Puede utilizar el Agente de Microsoft Office 365 para supervisar el estado y el rendimiento de los recursos de Office 365, como por ejemplo los servicios suscritos de Office 365, el portal de Office 365, los usuarios del buzón, sitios de SharePoint y almacenamiento OneDrive.

Monitoring Agent for NetApp Storage

Puede utilizar el Agente de NetApp Storage para supervisar el estado, disponibilidad y rendimiento de los sistemas de almacenamiento de NetApp mediante el OCUM (OnCommand Unified Manager) de NetApp. El agente de supervisión realiza las tareas siguientes:

- Identifica objetos del sistema de almacenamiento de rendimiento pobre
- Realiza el descubrimiento y la supervisión utilizando el servidor OCUM en el punto focal

Monitoring Agent for RabbitMQ

Puede utilizar el Agente de RabbitMQ para supervisar el estado y el rendimiento de los recursos de clúster de RabbitMQ, como por ejemplo los nodos, colas y canales del clúster.

Recopiladores de datos para aplicaciones Bluemix

Puede utilizar los recopiladores de datos de aplicaciones Bluemix para supervisar el estado y el rendimiento de los siguientes tipos de aplicaciones en Bluemix:

- Aplicaciones Liberty
- Aplicaciones Node.js
- Aplicaciones Python
- Aplicaciones Ruby

Puede ver datos de supervisión de recursos y de diagnóstico, como por ejemplo la utilización de recursos, el rendimiento e información detallada acerca de solicitudes y métodos.

Monitoring Agent for Siebel

Puede utilizar el Agente de Siebel para supervisar el estado y rendimiento de los recursos de Siebel, que incluyen estadísticas de Siebel, sesiones de usuario, componentes, tareas, servidor de la aplicaciones, Servidor de nombres de pasarela de Siebel, uso de memoria y CPU de proceso y supervisión de sucesos de registro.

Mejoras en los agentes

Monitoring Agent for Amazon EC2

Se han añadido las mejoras siguientes al Agente de Amazon EC2:

- Sustituir ID de instancia por nombre de etiqueta cuando está disponible un nombre de etiqueta
- Permitir filtrar y agrupar datos en función del nombre de etiqueta

Monitoring Agent for Db2

Se han añadido las mejoras siguientes al Agente de Hadoop:

- Linux on Power Little Endian (pLinux LE) está soportado
- Se ha añadido un archivo de script para otorgar privilegios a un usuario Db2 para ver los datos de todos los atributos del agente de Db2 para una instancia supervisada

Monitoring Agent for Hadoop

Se han añadido las mejoras siguientes al Agente de Hadoop:

- Se ha añadido soporte para instalar y configurar el agente en sistemas Windows 2016 y AIX 7.2
- Se ha añadido soporte para supervisar las siguientes ofertas de Hadoop: Hortonworks HDP 2.5, Cloudera CDH 5.6, 5.7 y 5.8, e IBM BigInsights 4.2
- Se ha añadido el botón de probar conexión para verificar la conexión con los daemons de Hadoop que especifique al configurar el agente
- Se ha mejorado el proceso de configuración del agente para reducir el tiempo y la complejidad de la configuración. La configuración se ha simplificado debido a que las siguientes tareas de requisito previo configuración ya no son necesarias:
  - Instalar el plug-in en cada nodo del clúster Hadoop
  - Configurar y actualizar el archivo `hadoop-metrics2.properties`
  - Reiniciar los daemons de Hadoop después de configurar el archivo `hadoop-metrics2.properties`
  - Configurar todos los DataNodes y NodeManagers del clúster
  - Reiniciar el agente cuando se añaden nodos adicionales al clúster

Monitoring Agent for JBoss

Se han añadido las mejoras siguientes al Agente de JBoss:

- Se ha añadido el rastreo de transacciones y la supervisión en profundidad a la oferta Advanced Agents
- Se ha añadido una página del panel de instrumentos para supervisar métricas de origen de datos
- Se ha añadido soporte para supervisar las siguientes ofertas de JBoss: WildFly 8.x/9.x/10.x, JBoss EAP 7.x, JBoss AS 7.x
- Se ha añadido soporte para ejecutar el agente en el sistema operativo Windows

Monitoring Agent for Linux KVM

Se han añadido las mejoras siguientes al panel de instrumentos del Agente de Linux KVM:

- Se ha actualizado el widget de grupo Hosts en la página Hosts, Clústeres y Almacenamiento para visualizar los ICR Memoria de planificación máxima (GB) e Instantánea en directo
- Se ha añadido la página Detalles de almacenamiento para visualizar detalles acerca de los discos e instantáneas de disco de la agrupación de almacenamiento
- Se ha añadido el widget de grupo Datos transmitidos/recibidos de red (GB) a la página Detalles de host para visualizar información histórica del total de datos (en GB) transmitidos y recibidos a través de la red

Monitoring Agent for Linux OS

Se ha añadido la mejora siguiente al Agente de sistema operativo Linux:

- Linux on Power Little Endian (pLinux LE) está soportado

Monitoring Agent for Microsoft Exchange Server

Se han añadido las mejoras siguientes al panel de instrumentos del Agente de Microsoft Exchange Server:

- Se han añadido los atributos de tiempo de entrada y tiempo de salida al conjunto de datos Accesibilidad.
- Se han añadido páginas y widgets de grupo para visualizar detalles de accesibilidad
- Se ha añadido un umbral de sucesos para la accesibilidad
- Se ha añadido soporte para instalar y configurar el agente en el sistema Exchange Server 2016 y Windows Server 2016

Monitoring Agent for Microsoft Internet Information Services

Se ha añadido la mejora siguiente al Agente de Microsoft IIS:

- Se ha añadido soporte para instalar y configurar el agente en el sistema Microsoft Windows Server 2016

Monitoring Agent for Microsoft Active Directory

Se han añadido las mejoras siguientes al Agente de Microsoft Active Directory:

- Se ha añadido widgets de grupo y páginas para visualizar los detalles de Objeto de política de grupo, Inicio de sesión de red, Autoridad de seguridad local y LDAP
- Se han añadido los siguientes conjuntos de datos, que puede ver en la pestaña **Detalles de atributo**:
  - Conjunto de datos de servicio
  - Réplica
  - Servicio de réplica de archivos
  - Unidad organizativa movida o suprimida
  - Atributos de LDAP
  - Gestor de cuentas de seguridad
  - DFS
  - Libreta de direcciones
  - Registro de sucesos
  - Objetos de establecimiento de contraseña
- Se han añadido los conjuntos de datos para ADFS, Proxy ADFS y Cola de hebra asíncrona
- Se ha añadido los widgets de grupo y páginas para visualizar detalles de ADFS y Proxy ADFS
- Se ha añadido soporte para instalar y configurar el agente en sistemas Windows Server 2016

Monitoring Agent for Microsoft .NET

Se han añadido las mejoras siguientes al panel de instrumentos del Agente de Microsoft .NET:

- Se ha actualizado el widget de grupo Estado de MS .NET de la página Componente para visualizar los tiempos de respuesta de llamadas a base de datos, el estado de los procesos .NET con un número de hebras elevado y las anomalías de compilación Just in Time (JIT)
- Se han añadido conjuntos de datos, páginas y widgets de grupo para mostrar detalles de compilación JIT, detalles de llamada a base de datos, descriptores de contexto de GC y recopilación de objetos fijados para un proceso .NET seleccionado, tasa de contienda de hebras y longitud de cola de hebra
- Se han añadido umbrales de sucesos para anomalías de JIT, anomalías de solicitud .NET, mandatos lentos, recogida de basura y las hebras activas en procesos .NET

Monitoring Agent for Microsoft SQL Server

Se han añadido las mejoras siguientes al panel de instrumentos del Agente de Microsoft SQL Server:

- Se ha añadido el widget de grupo Consultas costosas a la página Rendimiento del servidor - Detalle para visualizar los 10 planes de consulta principales almacenados en memoria caché de acuerdo con las estadísticas de rendimiento de Microsoft SQL Server
- Se ha añadido soporte para supervisar Microsoft SQL Server 2016
- Se ha añadido soporte para instalar y configurar el Agente de Microsoft SQL Server en el sistema Microsoft Windows Server 2016
- Se ha añadido la variable de entorno *COLL_ERRORLOG_RECYCLE_WAIT* para establecer el intervalo de tiempo (en segundos) durante el que el agente espera antes de recopilar datos del grupo de atributos Detalles de sucesos de error de MS SQL.

Monitoring Agent for MongoDB

Se han añadido las mejoras siguientes al panel de instrumentos del Agente de MongoDB:

- Se ha actualizado la página Componente para visualizar el número de instancias de MongoDB y su estado
- Se han añadido páginas para visualizar detalles de los motores de almacenamiento MMAPv1 y WiredTiger
- Se ha añadido la página Información de entrada y salida para visualizar detalles de cursor y datos históricos para las operaciones en cola, conexiones activas, flujo de datos y el acceso a datos del host seleccionado
- Se han añadido páginas para visualizar detalles de los bloqueos de las versiones 2.x y 3.x o posteriores
- Se ha añadido la página Detalles de réplica para visualizar detalles del miembro de réplica, oplog, y datos históricos del retardo de réplica y del espacio utilizado por oplog

Monitoring Agent for Node.js

Se han añadido las mejoras siguientes al Agente de Node.js para utilizar Métricas de aplicación de nodo (Appmetrics):

- Se ha añadido nuevos widgets de grupo y de panel de instrumentos para ver detalles de recogida de basura
- Se ha añadido nuevos widgets de grupo y de panel de instrumentos para ver detalles de bucle de sucesos

Monitoring Agent for PostgreSQL

Se han añadido las mejoras siguientes al Agente de PostgreSQL:

- Se ha añadido soporte para instalar y configurar el agente en sistemas Windows
- Se ha añadido soporte para supervisar PostgreSQL V9.6
- Se ha actualizado la página Visión general de estado, de modo que el estado no sea crítico cuando el índice de coincidencias del almacenamiento intermedio sea cero

Monitoring Agent for SAP NetWeaver Java Stack

Se han añadido las mejoras siguientes al Agente de SAP NetWeaver Java Stack:

- Se han añadido conjuntos de datos, widgets de grupo y páginas para recopilar y ver los datos de diagnóstico y rastreo de transacciones
- Se ha añadido soporte para instalar y configurar el agente en sistemas Windows 2016

Monitoring Agent for Synthetic Playback

Se ha añadido la mejora siguiente al Agente de Synthetic Playback:

- El Agente de Synthetic Playback incluye una nueva función de filtrado para transacciones sintéticas. En el Gestor de scripts sintéticos, configure listas negras y blancas para las transacciones sintéticas que excluyan o incluyan solicitudes a URL y dominios especificados. Utilice las listas negras y las listas blancas para filtrar o incluir dependencias que afectan a los tiempos de respuesta de la aplicación, como por ejemplo mediciones de terceros.

Monitoring Agent for Tomcat

Se ha añadido la mejora siguiente al Agente de Tomcat:

- Se ha añadido soporte para instalar y configurar el Agente de Tomcat en sistemas Windows y SUSE Linux Enterprise 12

Monitoring Agent for WebSphere Applications

e han añadido las mejoras siguientes al Agente de WebSphere Applications:

- Linux on Power Little Endian (pLinux LE) está soportado. (El rastreo de transacciones no está soportado en sistemas pLinux LE.)
- Se ha añadido soporte para IBM WebSphere Application Server tradicional V9.
- Se ha añadido el panel de instrumentos Análisis de memoria para diagnosticar posibles pérdidas de memoria comprobando la información de uso del almacenamiento dinámico de cada volcado de almacenamiento dinámico. Debe habilitarse la modalidad de diagnóstico para que este panel de instrumentos contenga datos.
- Se ha añadido soporte para utilizar el conjunto de datos Estado de salud de la aplicación para crear umbrales de sucesos para la supervisión del estado de la aplicación. La recopilación de datos para este uso está inhabilitada de forma predeterminada. Debe modificar el archivo de propiedades del recopilador de datos para habilitarla antes de crear umbrales de sucesos.
- Se ha simplificado la configuración manual del recopilador de datos. Para WebSphere Applications Server, sólo necesita añadir algunos argumentos y variables de la JVM para el servidor de aplicaciones en la consola administrativa de WebSphere. Para Liberty, sólo es necesario modificar tres archivos para el servidor.

Agente de Supervisión de tiempo de respuesta

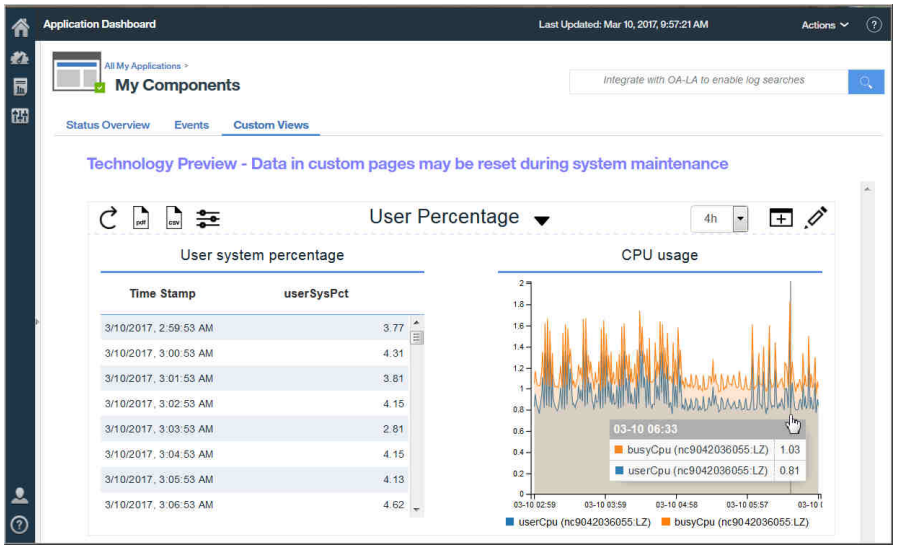
Se han añadido las mejoras siguientes al Agente de Supervisión de tiempo de respuesta:

- Se ha añadido soporte para configurar el seguimiento de usuarios para aplicaciones en la página **Configuración de agente**.
- Se ha añadido soporte para configurar el seguimiento de sesiones para aplicaciones en la página **Configuración**.

Mejoras del Consola de Cloud APM

Se han realizado diversas mejoras en las interfaces de instalación y configuración del agente, así como las siguientes mejoras en la consola:

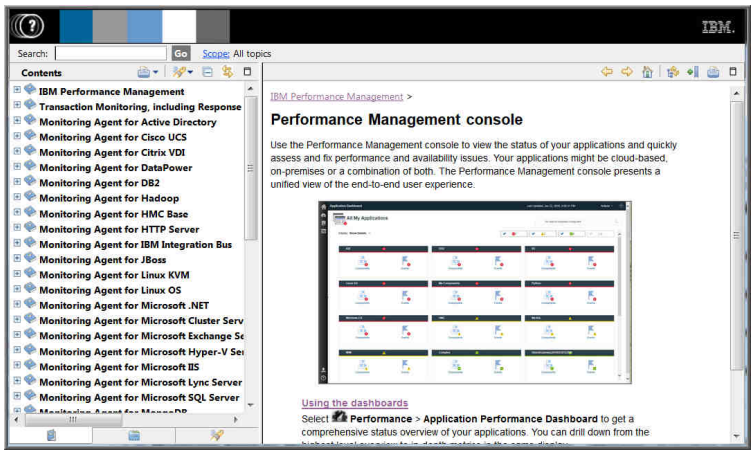
- Avance tecnológico: una nueva pestaña **Vistas personalizadas** está disponible para las páginas del Panel de instrumentos de aplicaciones. Puede crear diversas vistas de medidas de informes a partir de un recurso gestionado y aplicar funciones tales como promedio y recuento. Tras abrir una página guardada, puede renovar la página con datos de un recurso diferente y descargar las medidas de página como un archivo PDF o CSV. Para obtener más información, consulte, consulte “Vistas personalizadas” en la página 1147.



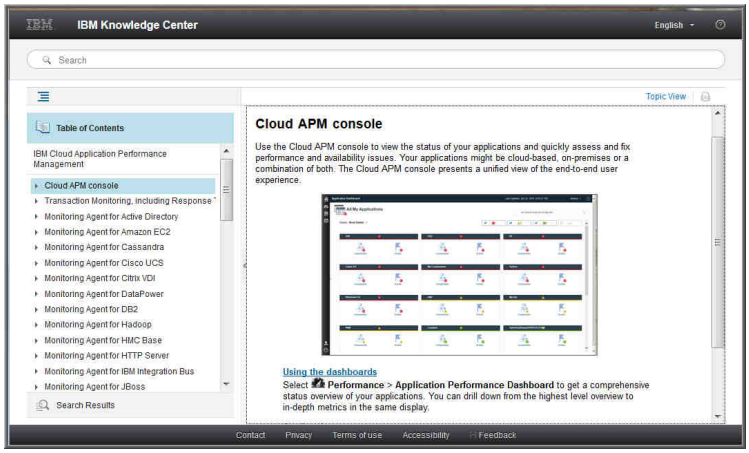
Si no visualiza **Vistas personalizadas** en la suscripción de Cloud APM y desea probar esta nueva función, abra una petición de servicio con Soporte de IBM para habilitar el avance tecnológico **Vistas personalizadas**. Tenga en cuenta que las páginas personalizadas de panel de instrumentos y los datos históricos que los llenan no se guardan durante el mantenimiento del sistema.

- Al abrir el sistema de ayuda de la Consola de Cloud APM, observe que está alojado en IBM Knowledge Center. Dispone de la herramienta **Ocultar tabla de contenidos**, funciones de búsqueda e impresión y enlaces a información de soporte y opciones de comentario.

Antes de



Después de



Mejoras en Agent Builder

Se ha mejorado el soporte para crear paneles de instrumentos de resumen de Cloud APM para los agentes de Agent Builder. Debe utilizar conjuntos de datos de fila única para suministrar datos a los

paneles de instrumentos de resumen. Puede proporcionar dichos conjuntos de datos desde archivos de registro completos y desde cualquier conjunto de datos pueda filtrarse para generar una sola fila.

Novedades: septiembre de 2016

Hay características, prestaciones y cobertura nuevas disponibles en el release de septiembre de 2016 de Performance Management on Cloud.

Nuevos agentes disponibles

Monitoring Agent for Amazon EC2
Puede utilizar Agente de Amazon EC2 para supervisar el estado, disponibilidad y rendimiento de Amazon Elastic Compute Cloud (EC2) Recursos de instancia. Puede supervisar los recursos siguientes:

- Uso de CPU
- Utilización de EBS (Elastic Block Store)
- Utilización de red
- Actualizaciones de mantenimiento de AWS (Amazon Web Services)
- Rendimiento de disco

Este agente se encuentra en Infrastructure Extension Pack y está disponible para las ofertas siguientes: IBM Monitoring, IBM Application Performance Management e IBM Application Performance Management Advanced.

Monitoring Agent for SAP NetWeaver Java Stack
Puede utilizar el Agente de SAP NetWeaver Java Stack para supervisar el estado, la disponibilidad y el rendimiento de su clúster de pila Java de SAP NetWeaver y recursos de instancia. Puede utilizar el agente para supervisar los recursos del clúster como, por ejemplo, volcados de almacenamiento dinámico, la instancia de la JVM, el tiempo de respuesta de las sesiones de usuario, detalles de transacción, información del sistema y detalles de licencia. Puede utilizar el agente para supervisar los recursos de la instancia como, por ejemplo, la utilización de CPU, el uso del disco, el uso de la memoria, la colección de base de datos, la recogida de basura, los volcados de almacenamiento dinámico, la aplicación que ha fallado, el contenedor web e información de sesión. Este agente se encuentra en Advanced Extension Pack y está disponible si tiene una de las ofertas siguientes: IBM Application Performance Management e IBM Application Performance Management Advanced.

Mejoras en el agente

Monitoring Agent for Citrix Virtual Desktop Infrastructure
Se ha añadido la posibilidad de recuperar sucesos de registro de sucesos de Windows para máquinas de Virtual Delivery Agent (VDA) y Desktop Delivery Controller (DDC).

Monitoring Agent for Linux KVM
Los paneles de instrumentos están disponibles para que el agente supervise el despliegue de las máquinas virtuales basadas en el kernel de Linux. Los paneles de instrumentos proporcionan las prestaciones siguientes de supervisión:

- El panel de instrumentos de resumen muestra el estado general de los hosts basándose en el uso de la CPU y memoria del entorno o la aplicación de las máquinas virtuales basadas en el kernel de Linux.
- El panel de instrumentos Detalle de host muestra detalles sobre el host seleccionado.
- El panel de instrumentos Hosts, Clústeres y Almacenamiento muestra detalles sobre las máquinas virtuales supervisadas.
- El panel de instrumentos Detalles de máquina virtual muestra detalles sobre la máquina virtual que seleccione en la página Detalle de host.

Monitoring Agent for Linux OS

Docker V1.8.0 o posterior está soportado. Se han añadido nuevos grupos de atributos y widgets para permitir que el agente de sistema operativo Linux proporcione prestaciones de supervisión de Docker.

Monitoring Agent for Oracle Database

El panel de instrumentos del agente de la agente de base de datos Oracle incluye las nuevas características siguientes en la página Detalles de instancia:

- Una tabla que muestra información sobre la contención de bloqueo en la instancia seleccionada.
- Una tabla que muestra información sobre Oracle Real Application Clusters GCS y GES.
- Una tabla que muestra detalles de los grupos de discos ASM (Automatic Storage Management) que están conectados a la instancia seleccionada.
- Una vista que muestra información detallada por espacio de tabla, que es visible si pulsa **Últimos 5 espacios de tabla libres**.
- Una tabla que muestra los detalles históricos de los procesos en primer plano y en segundo plano que están conectados a la instancia seleccionada. Puede pulsar la entidad en la tabla y ver una tabla detallada de todos los procesos para dicha instancia.
- Una tabla que muestra las Peores 5 consultas SQL (por tiempo de ejecución) en la instancia seleccionada. Puede pulsar en la tabla y ver una tabla detallada de las 50 peores consultas SQL para dicha instancia.

Monitoring Agent for Synthetic Playback

El Agente de Synthetic Playback incluye una nueva característica de seguridad. Puede impedir que las contraseñas almacenadas en scripts sintéticos se visualicen en el Gestor de scripts sintéticos.

Monitoring Agent for VMware VI

Con la adición de la característica de agente de desacoplamiento de agente, puede visualizar y seleccionar el nodo de agente y sus subnodos en la misma vista.

Al seleccionar el componente Infraestructura virtual de VMware en la ventana Seleccionar componente, el editor de componentes muestra una estructura de árbol del nodo de agente con todos sus subnodos.

- Si expande el árbol y selecciona el nodo de agente, todos los subnodos se seleccionan automáticamente. También puede expandir el árbol y seleccionar individualmente los subnodos que desee supervisar.
- Si selecciona el nodo de agente cuando el árbol está contraído, todos los subnodos se excluyen automáticamente.

Cuando se selecciona el componente de servidor ESX en la ventana Seleccionar componente, junto con subnodos, los servidores ESX autónomos también se muestran en el editor de componentes. Con los subnodos, puede seleccionar servidores ESX autónomos para la supervisión.

Una vez que se ha creado la aplicación, el panel de instrumentos de IU APM muestra una estructura de árbol de la instancia del agente como padre y sus nodos como hijos.

Agente de Supervisión de tiempo de respuesta

Puede personalizar las ubicaciones que se aplican a rangos de direcciones o direcciones IP específicas en los paneles de instrumentos Transacciones de usuario final. Utilice la pestaña **Geolocalización** en la **Configuración de agente** para personalizar los valores de ubicación.

Mejoras del Consola de Cloud APM

- Se han realizado diversas mejoras en la instalación del agente y las interfaces de configuración.
- Se ha añadido una opción **Registro de panel de instrumentos** al menú **Acciones** para revisar la lista de paneles de instrumentos de agente que se han actualizado desde el último reinicio de servidor.

Para obtener más información, consulte "Todas mis aplicaciones – Panel de instrumentos del rendimiento de aplicaciones" en la página 1113.

- La página Panel de instrumentos del rendimiento de aplicaciones para la aplicación seleccionada se ha mejorado para obtener una mejor visualización. Se muestra un recuento de sucesos de gravedad crítica y de aviso en el título de pestaña Sucesos y sustituye el diagrama de barras **Resumen de gravedad de sucesos**. Para aplicaciones con las vistas de topología habilitadas, la vista **Topología de aplicación de agregado** tiene un botón de conmutador para cambiar al diagrama de barras Estado de componente actual. Para obtener más información, consulte "Visión general de estado" en la página 1116.
- En releases anteriores, la pestaña Panel de instrumentos del rendimiento de aplicaciones **Detalles de atributos** estaba disponible únicamente para instancias de componentes. La pestaña **Detalles de atributo** está disponible para crear tablas históricas de instancias de transacciones de Agente de Supervisión de tiempo de respuesta y Agente de Synthetic Playback. Para los usuarios con discapacidad visual, la posibilidad de crear tablas históricas proporciona una alternativa a los diagramas de líneas, que las tecnologías de asistencia, como el software lector de pantalla no puede interpretar. Para obtener más información, consulte "Visualización y gestión de gráficos y tablas personalizados" en la página 1127.

API

Puede utilizar APIs para crear scripts para automatizar la incorporación de su entorno de Performance Management. Para obtener más información, consulte "Exploración de las API" en la página 1107.

Novedades: abril de 2016

Hay características, prestaciones y cobertura nuevas disponibles en el release de abril de 2016 de Performance Management on Cloud.

IBM Marketplace

Las ofertas de IBM Performance Management on Cloud están disponibles desde IBM Marketplace. Inicie sesión para una prueba gratuita o su cuenta de suscripción. Para obtener más información, consulte "Descarga de los agentes y recopiladores de datos" en la página 107.

Nuevos agentes disponibles

Monitoring Agent for Citrix Virtual Desktop Infrastructure

Puede utilizar el Agente de Citrix VDI para supervisar el estado, la disponibilidad y el rendimiento de Citrix XenDesktop o los recursos XenApp como sitios, máquinas, aplicaciones, escritorios, sesiones y usuarios. Este agente se encuentra en Infrastructure Extension Pack y está disponible para las ofertas siguientes: IBM Monitoring, IBM Application Performance Management e IBM Application Performance Management Advanced.

Monitoring Agent for Skype for Business Server

Puede utilizar el Agente de Skype for Business Server para supervisar el estado, la disponibilidad y el rendimiento de los recursos de Microsoft Lync Server tales como base de datos, servidor de mediación, transacciones sintéticas, mensajería instantánea, operaciones de grabación de servicio CDR e iguales SIP.

Monitoring Agent for WebLogic

Puede utilizar el Agente de WebLogic para supervisar el estado, la disponibilidad y el rendimiento de recursos de servidor WebLogic como máquinas virtuales Java (JVM), servicio de mensajería Java (JMS) y Java Database Connectivity (JDBC).

Mejoras en la integración

Coexistencia de agentes

Se da soporte a la coexistencia de agentes. Puede instalar agentes de IBM Performance Management en el mismo sistema donde están instalados los agentes de IBM Tivoli Monitoring. Sin embargo, no se pueden instalar ambos agentes en el mismo directorio. Consulte "Coexistencia del agente de Cloud APM y el agente de Tivoli Monitoring" en la página 984.

IBM Alert Notification
Alert Notification incluye una aplicación móvil que ofrece un subconjunto de funciones de notificación de alertas en dispositivos iOS y Android.

Supervisión de Pila de integración de IBM
Puede supervisar la Pila de integración de IBM para ver la información de rastreo de transacciones para los productos middleware de dispositivo IBM MQ, IBM Integration Bus y DataPower, y los servicios que exponen y resolver problemas si surge alguno. Consulte "Escenario: Supervisión de la Pila de integración de IBM" en la página 101.

Mejoras en el agente

Monitoring Agent for Db2
Se han añadido mandatos para otorgar privilegios al usuario predeterminado (para sistemas Windows) y al usuario propietario de la instancia (para sistemas Linux y AIX) para ver los datos de algunos de los atributos del Agente de Db2.

Monitoring Agent for Hadoop
El Agente de Hadoop está soportado en sistemas operativos Linux, Windows y AIX.

Monitoring Agent for HMC Base
Se proporcionan prestaciones de supervisión para entrada/salida virtual y para sucesos de hardware.

Monitoring Agent for IBM Integration Bus

La vía de acceso a biblioteca de la versión más reciente de IBM MQ (WebSphere MQ) se puede descubrir automáticamente durante la configuración de agente en sistemas Linux y AIX.

Monitoring Agent for Microsoft Cluster Server
El Agente de Microsoft Cluster Server se configura automáticamente una vez instalado.

Monitoring Agent for Microsoft Exchange Server
Se han añadido algunos servicios adicionales en la pestaña **Servicios de Exchange** de la ventana de configuración del agente para determinar el estado del Servidor de Exchange.

Monitoring Agent for Microsoft Hyper-V Server
Se ha eliminado el panel de configuración del agente. No es necesaria la configuración de agente.

Monitoring Agent for SAP HANA Database
Se ha añadido el widget de grupo Detalles de información de memoria caché en el panel de instrumentos **Detalles de base de datos de SAP HANA** para proporcionar información sobre el porcentaje de memoria utilizada, porcentaje de memoria disponible y la proporción de aciertos de la memoria caché para la base de datos supervisada.

Monitoring Agent for Synthetic Playback
El Agente de Synthetic Playback incluye las características siguientes:

- Puede instalar y configurar el Agente de Synthetic Playback para supervisar el rendimiento y la disponibilidad de aplicaciones privadas e internas en el Panel de instrumentos del rendimiento de aplicaciones, además de aplicaciones públicas y externas.
- Utilice el Gestor de scripts sintéticos para generar un script simple para probar la disponibilidad y el rendimiento de las aplicaciones.
- Configure la reproducción simultánea o escalonada de transacciones sintéticas en ubicaciones distintas.
- Supervise el uso de reproducción mensual en el Gestor de scripts sintéticos.
- Vea métricas HTTP y proporciones de disponibilidad en informes de Agente de Synthetic Playback.
- Vea dos nuevos informes: Tendencia de transacciones y Tendencia de subtransacciones.
- Organice las transacciones sintéticas en un grupo de recursos y aplique umbrales a todas las transacciones en ese grupo de recursos.

- Vea datos de transacciones sintéticas en la ventana **Mis transacciones** en el Panel de instrumentos del rendimiento de aplicaciones sin tener que crear una aplicación que contenga transacciones sintéticas asociadas.
- Descargue scripts sintéticos desde el Gestor de scripts sintéticos.

Monitoring Agent for VMware VI

El panel de instrumentos del Agente de VMware VI se ha mejorado para incluir las siguientes características nuevas:

- El número de alarmas activadas en estado crítico o de aviso también se visualizan en la página **Componente**.
- Una tabla nueva en la página **Resumen de clúster** proporciona información sobre las alarmas proactivas y de anomalía. Puede pulsar la entidad activada en la tabla y ver la página de detalles de dicha entidad activada.
- Una tabla nueva en la página **Detalle de clúster** muestra detalles de los servidores ESX que pertenecen al clúster seleccionado. Puede pulsar el servidor ESX y ver la página de detalles de dicho servidor ESX.
- La tabla de almacén de datos en la página **Detalle de clúster** muestra la métrica de exceso de compromiso del almacén de datos.
- La tabla de máquinas virtuales en la página Detalle de máquina virtual muestra más medidas de rendimiento como el tamaño de memoria, NICs y discos. Puede pulsar estas métricas y ver sus páginas de detalles.
- Se han añadido nuevos widgets y páginas para visualizar métricas de rendimiento importantes de memoria, discos y red para la máquina virtual seleccionada.
- Una tabla nueva en la página **Detalle de servidor ESX** muestra el rendimiento de la red del servidor de red.
- La tabla de almacén de datos en la página **Detalle de VM** y la página **Detalle de servidor ESX** muestran la métrica de latencia del almacén de datos.
- Una tabla nueva en la página **Detalle del almacén de datos** muestra información acerca de la máquina virtual que está asociada con el almacén de datos. Puede pulsar la máquina virtual en la tabla y ver la página **Detalle de máquina virtual**.
- El título del gráfico % Memoria (Historial) en la página **Detalle de máquina virtual** se ha cambiado por Memoria huésped (Historial).

Monitoring Agent for WebSphere Applications

El panel de instrumentos de resumen de solicitudes en curso proporciona la posibilidad de identificar las instancias de solicitud actualmente lentas o que se han colgado. Puede realizar una operación de cancelación en una solicitud en curso seleccionando la solicitud y pulsando **Cancelar hebra** en el widget de solicitud en curso en este panel de instrumentos.

Todos los umbrales de sucesos predefinidos se han refinado para proporcionar una experiencia de usuario mejor. Las mejoras y actualizaciones están relacionadas con la condición que desencadena una alerta, el intervalo de muestreo y la gravedad del umbral.

La interfaz de usuario del Monitoring Agent for WebSphere Applications es accesible a usuarios con discapacidad física.

El proceso de configuración se ha refinado según los comentarios del cliente y revisiones técnicas para proporcionar una experiencia de usuario mejor.

Monitoring Agent for WebSphere MQ

Se han realizado algunos cambios en los umbrales de suceso predefinidos:

- Todos los umbrales predefinidos tienen el prefijo MQ_ en lugar de MQSeries_ de las versiones anteriores.
- Se han añadido dos umbrales, MQ_Channel_Initiator_Crit y MQ_Queue_Manager_Crit, para desencadenar alertas críticas para el estado del servidor de iniciador de canal y el estado del gestor de colas.

- La condición de desencadenante del suceso MQ_Queue_Depth_High se ha cambiado de 80% estático a un valor de profundidad alto de la cola.

El nombre del widget **Cola no en lectura – 5 principales** se ha cambiado a **Cola en uso no en lectura – 5 principales**. Este widget proporciona una lista de las cinco colas principales que tienen mensajes y están conectadas por una o más aplicaciones para poner mensajes en la cola, pero no las está leyendo ninguna aplicación.

La vía de acceso a biblioteca de la versión más reciente de IBM MQ (WebSphere MQ) se puede descubrir automáticamente durante la configuración de agente. Puede mantener el parámetro **WMQLIBPATH** vacío en el archivo de respuestas silencioso o aceptar el valor predeterminado cuando configura el agente de forma interactiva.

Agentes de sistema operativo

Los agentes de sistema contienen una nueva funcionalidad para supervisar archivos de registro de aplicación. La funcionalidad incluye la posibilidad de configurar la supervisión de archivo de registro basado en expresiones regulares.

Por compatibilidad, el agente de sistema operativo consume la siguiente información y formatos:

- Información de configuración y el archivo de formato que ha utilizado IBM Tivoli Monitoring 6.x Log File Agent
- Información de configuración y series de formato que ha utilizado Tivoli Event Console Log File Adapter

Estas series de formato permiten al agente filtrar los datos de registro de acuerdo con patrones en el archivo de formato y enviar sólo los datos relevantes a un consumidor de sucesos. El agente de sistema operativo envía datos al servidor de Performance Management o a través de Event Integration Facility (EIF) a cualquier receptor EIF, como el analizador de EIF OMNIbus.

Agente de Supervisión de tiempo de respuesta

Los paneles de instrumentos de transacciones de usuario final incluyen información de usuario y de dispositivo, que anteriormente se visualizaba en los paneles de instrumentos de Usuarios autenticados y Usuarios de dispositivos móviles en el grupo Usuarios. La información de usuario, sesión y dispositivo se clasifica por ubicación (país, estado y ciudad) basándose en la dirección IP del usuario. Utilice los paneles de instrumentos nuevos y actualizados para comprender los volúmenes de usuario y si hay problemas aislados para conjuntos específicos de usuarios.

Personalice las ubicaciones que se han aplicado a direcciones IP específicas o rangos de direcciones en los paneles de instrumentos Transacción de usuario final para su entorno concreto. Utilice la pestaña **Geolocalización** en la **Configuración de agente** para personalizar los valores de ubicación.

Rastreo de transacciones

La página Resumen de transacciones incluye una topología Dependencias de servicio que muestra el nodo de recursos seleccionado, como IBM Integration Bus, y los servicios de los que depende. La página Detalles de transacción incluye una topología Dependencias de transacción que muestra un nodo de transacciones para cada instancia de componente y un nodo no instrumentado para cada servicio dependiente a nivel de transacción, por ejemplo, IBM Integration Bus y sus transacciones de servicio. La página Detalles de transacción también resalta los usuarios de la aplicación seleccionada que están experimentando los tiempos de respuesta más lentos, y los host con mayor volumen de transacciones.

Mejoras del agente general

Se han realizado las siguientes mejoras en la instalación y configuración del agente general:

- El script de instalación de agente realiza una comprobación de permisos antes de que se inicie la instalación. Si no tiene los permisos adecuados, se visualiza un mensaje.
- El mandato de estado de agente comprueba el estado entre el agente y la consola de Performance Management.

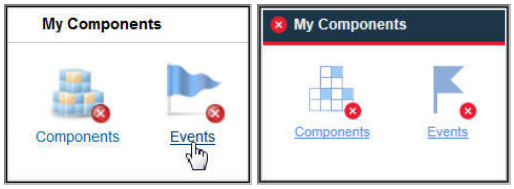
- Los agentes soportados en sistemas Windows tienen un programa de utilidad de interfaz gráfica de usuario que puede utilizar para realizar la configuración del agente y comprobar el estado de conexión.
- Puede utilizar un nuevo mandato para eliminar una instancia de agente sin desinstalar el agente.

Mejoras del servidor de Performance Management

La autenticación de usuario de Performance Management se gestiona mediante un proveedor de IBMid OpenID Connect.

Mejoras de la consola de Performance Management

- El aspecto de la consola de Performance Management se ha actualizado para alinearse con la interfaz de usuario de IBM Bluemix. Por ejemplo, vea las diferencias entre un cuadro de resumen en el panel de instrumentos de **Todas mis aplicaciones** de V8.1.2 y ahora:



- Se ha añadido una opción nueva a la página Configuración avanzada para que los usuarios avanzados puedan habilitar o inhabilitar fácilmente todos los umbrales predefinidos a través de todos los grupos de sistemas. Consulte “Información básica” en la página 1010.
- Se ha añadido una opción nueva a la página Configuración avanzada para controlar la velocidad de renovación automática del Panel de instrumentos del rendimiento de aplicaciones. Para obtener más información, consulte “Integración de interfaz de usuario” en la página 1108.
- Se han realizado diversas mejoras en la instalación del agente y las interfaces de configuración.
- Mejoras en la accesibilidad de la consola de Performance Management. Para obtener información sobre las características de accesibilidad de la interfaz de usuario, consulte “Funciones de accesibilidad” en la página 1549.

API

Puede utilizar APIs para crear scripts para automatizar la incorporación de su entorno de Performance Management. Para obtener más información, consulte “Exploración de las API” en la página 1107.

Mejora de Agent Builder

Agent Builder incluye un filtrado de conjunto de datos mejorado. Puede utilizar el filtrado para crear conjuntos de datos que devuelven una sola fila en función de los conjuntos de datos de varias filas incluido el conjunto de datos Disponibilidad. Utilice esta característica para proporcionar información en paneles de instrumentos de resumen.

Capítulo 2. Documentación en PDF

Los documentos en PDF están disponibles para los temas de esta colección de temas de IBM Knowledge Center y para las referencias de los agentes.

IBM Knowledge Center en formato PDF

Además de esta Guía del usuario, puede descargar IBM Agent Builder: Guía del usuario.

PDFs de referencia de agente

Para descargar la Referencia de un agente, consulte Agent metrics/Reference PDFs en Application Performance Management Developer Center. La Referencia proporciona información sobre paneles de instrumentos, umbrales de sucesos y conjuntos de datos. Los conjuntos de datos contienen atributos, que son métricas que ha notificado el agente y que componen los indicadores clave de rendimiento (ICR). Puede encontrar la versión del agente en la página de título del archivo PDF.

Capítulo 3. Visión general del producto

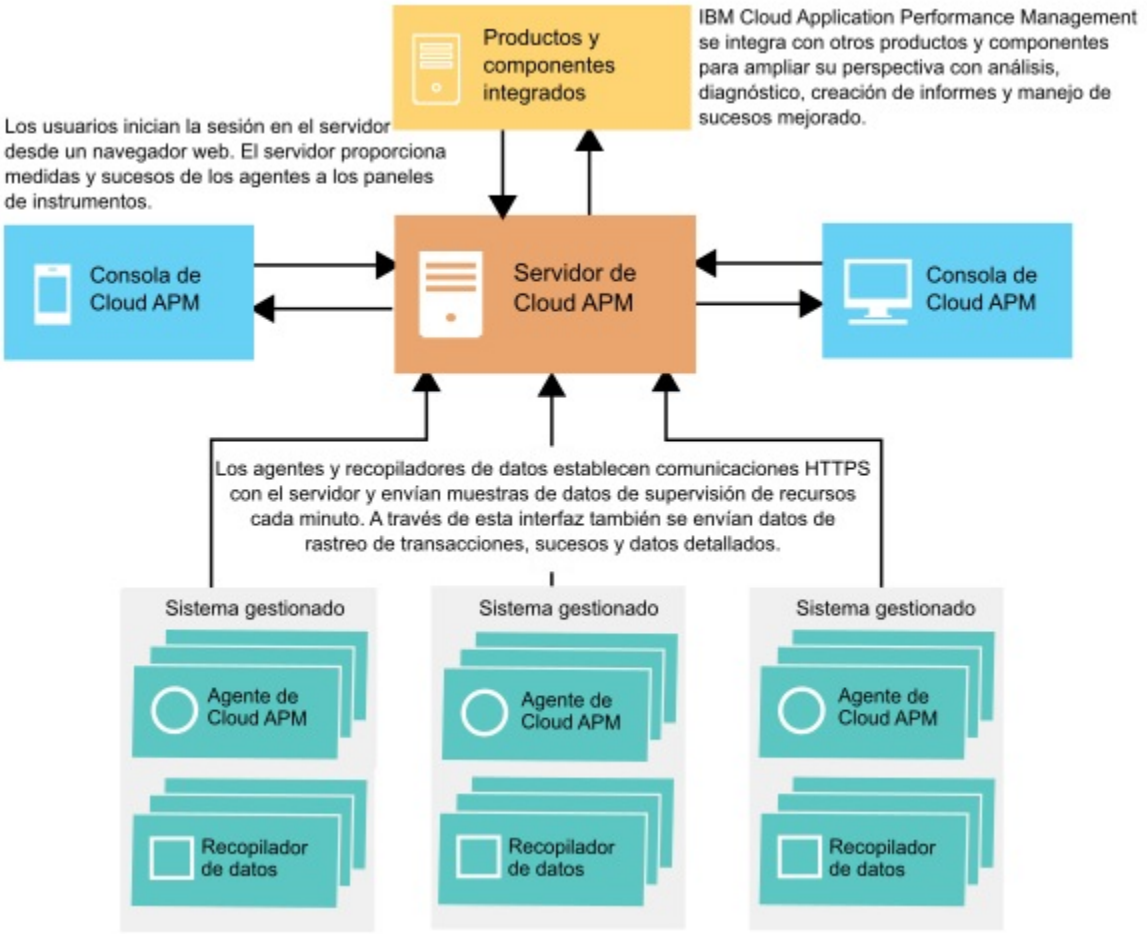
IBM Cloud Application Performance Management (Cloud APM) es una solución global que le ayuda a gestionar el rendimiento y la disponibilidad de aplicaciones que se han desplegado en instalaciones locales (privado), en una nube pública, o como una combinación híbrida. Esta solución le proporciona visibilidad, control y automatización para sus aplicaciones y garantiza un rendimiento óptimo y un uso eficaz de los recursos.

Mediante esta solución, puede gestionar el centro de datos, la infraestructura de nube y las cargas de trabajo con inteligencia cognitiva. Puede reducir y evitar interrupciones y retrasos en un mundo de aplicación híbrida ya que Cloud APM le ayudará a pasar de identificar problemas de rendimiento a aislar donde el problema está ocurriendo, y a diagnosticar los problemas antes de que la empresa se vea afectada.

Utilice las funciones clave que varían por oferta, para trabajar con datos recopilados por los agentes y recopiladores de datos de Cloud APM. Hay más funciones disponibles por medio de la integración con otros productos y componentes.

Visión general de la arquitectura

IBM Cloud Application Performance Management utiliza *agentes* y *recopiladores de datos* para recopilar los datos de los host supervisados. Los agentes y recopiladores de datos pasan los datos al Servidor de Cloud APM, que los intercala en la Consola de Cloud APM. El Servidor de Cloud APM está alojado en la nube de IBM.



Recopilación de datos

Los agentes y recopiladores de datos supervisan sistemas, subsistemas o aplicaciones y recopilan los datos. Un agente o un recopilador de datos interactúa con un recurso único (por ejemplo, un sistema o una aplicación) y, en la mayoría de los casos, está en el mismo sistema o máquina virtual donde se ejecuta el sistema o la aplicación. Por ejemplo, el Agente de sistema operativo Linux recopila los indicadores de rendimiento del sistema operativo en el host Linux y el Agente de WebSphere Applications supervisa los indicadores de rendimiento de los servidores de aplicaciones WebSphere. Además, algunos agentes efectúan el rastreo de transacciones entre distintos recursos.

Puede configurar umbrales en los indicadores clave de rendimiento (ICR). Si un indicador cambia para situarse por encima o por bajo del umbral, el agente o recopilador de datos genera una alerta, que el servidor procesa. También puede configurar el envío de sucesos a un destino como, por ejemplo, Netcool/OMNIbus Probe for Tivoli EIF o un servidor SMTP y utilizar Alert Notification para configurar notificaciones por correo electrónico para sucesos.

Los agentes y recopiladores de datos están preconfigurados para comunicarse con el Servidor de Cloud APM.

Comunicación entre el servidor y los agentes o recopiladores de datos

Los agentes y recopiladores de datos en cada uno de los hosts supervisados establecen una comunicación HTTPS con el Servidor de Cloud APM, que está en la nube de IBM. El agente o el recopilador de datos es el lado del cliente de la conexión.

Los agentes y los recopiladores de datos requieren conectividad a Internet para enviar datos al servidor y, si no pueden enviar datos directamente a través de Internet, podría ser necesario un proxy directo. Para obtener más información, consulte “Conectividad de red” en la página 165.

Datos almacenados por el servidor

Los agentes y los recopiladores de datos envían datos al Servidor de Cloud APM a intervalos que van de 1 minuto a 8 minutos en función del tipo de datos. El servidor almacena todos los valores enviados por los agentes y recopiladores de datos durante 8 días de forma predeterminada. Los datos de transacciones resumidos se almacenan durante periodos más largos.

Los datos de supervisión guardados se denominan datos *históricos*. El servidor utiliza los datos históricos para mostrar las tablas y gráficos que puede utilizar para analizar las tendencias del entorno.

También están disponibles los informes históricos para determinados agentes. Para obtener más información, consulte “Informes” en la página 1158.

Escalabilidad

Puede supervisar hasta 10.000 sistemas gestionados desde Cloud APM. Un sistema gestionado es un solo sistema operativo, subsistema o aplicación en su empresa que un agente está supervisando.

Cloud APM admite entre 150 y 400 transacciones de usuario supervisadas por segundo.

Integración

IBM Cloud Application Performance Management se integra con otros productos y componentes si se han configurado para la comunicación con el Servidor de Cloud APM.

Los productos que se pueden integrar incluyen IBM Control Desk, Netcool/OMNIbus, Tivoli Monitoring, OMEGAMON, Operations Analytics - Log Analysis, Operations Analytics - Predictive Insights, IBM Alert Notification e IBM Cloud.

Agent Builder es un componente que se puede utilizar para crear agentes personalizados.

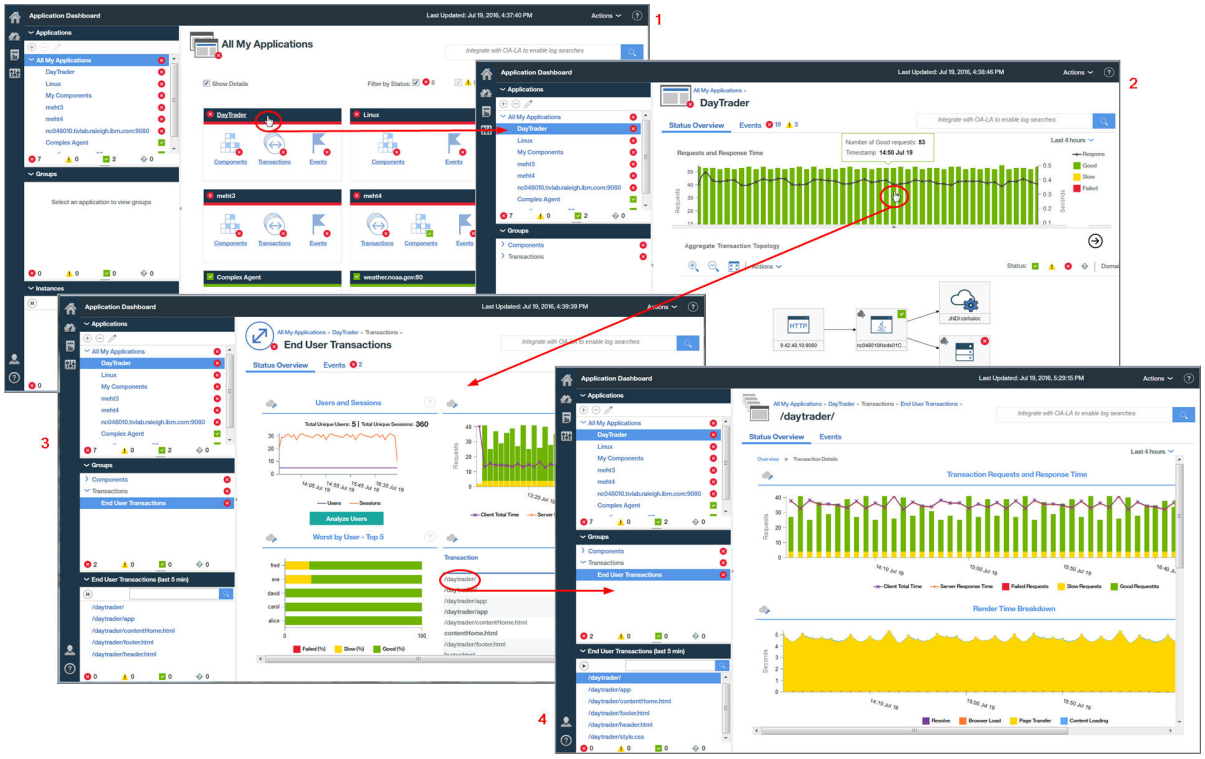
Interfaz de usuario

La Consola de Cloud APM es la interfaz de usuario para Cloud APM. Esta interfaz de usuario unificada proporciona una vista única entre aplicaciones híbridas. Puede utilizar la consola para visualizar el estado de las aplicaciones y evaluar y corregir rápidamente los problemas de rendimiento y disponibilidad.

Los paneles de instrumentos en la consola simplifican la identificación de problemas, para poder aislar los cuellos de botella que afectan al rendimiento de la aplicación. Con una navegación sencilla por el panel de instrumentos, puede pasar de una vista del estado de la aplicación al detalle a nivel de código. Tiene visibilidad de problemas de código fuente en el momento exacto de un problema. Puede buscar y diagnosticar problemas mediante el análisis de búsqueda integrada.

El navegador de Panel de instrumentos del rendimiento de aplicaciones en la consola es jerárquico, lo que proporciona una visión general del estado de las aplicaciones, el estado de sus componentes y la calidad de la experiencia del usuario. Si desea más detalles sobre el recurso supervisado, puede pulsar un elemento del navegador o un enlace en las vistas del panel de instrumentos. Considere, por ejemplo, que la aplicación tiene un tiempo de respuesta lento. El problema se ve en el panel de instrumentos. Empezando en el panel de instrumentos, puede seguir el problema hasta su origen pulsando los enlaces para descubrir la causa: utilización alta de CPU en un sistema debido a un proceso descontrolado.

Para obtener más información sobre cómo utilizar los paneles de instrumentos en la Consola de Cloud APM, consulte Capítulo 10, “Utilización de los paneles de instrumentos”, en la página 1113.



Ofertas y complementos

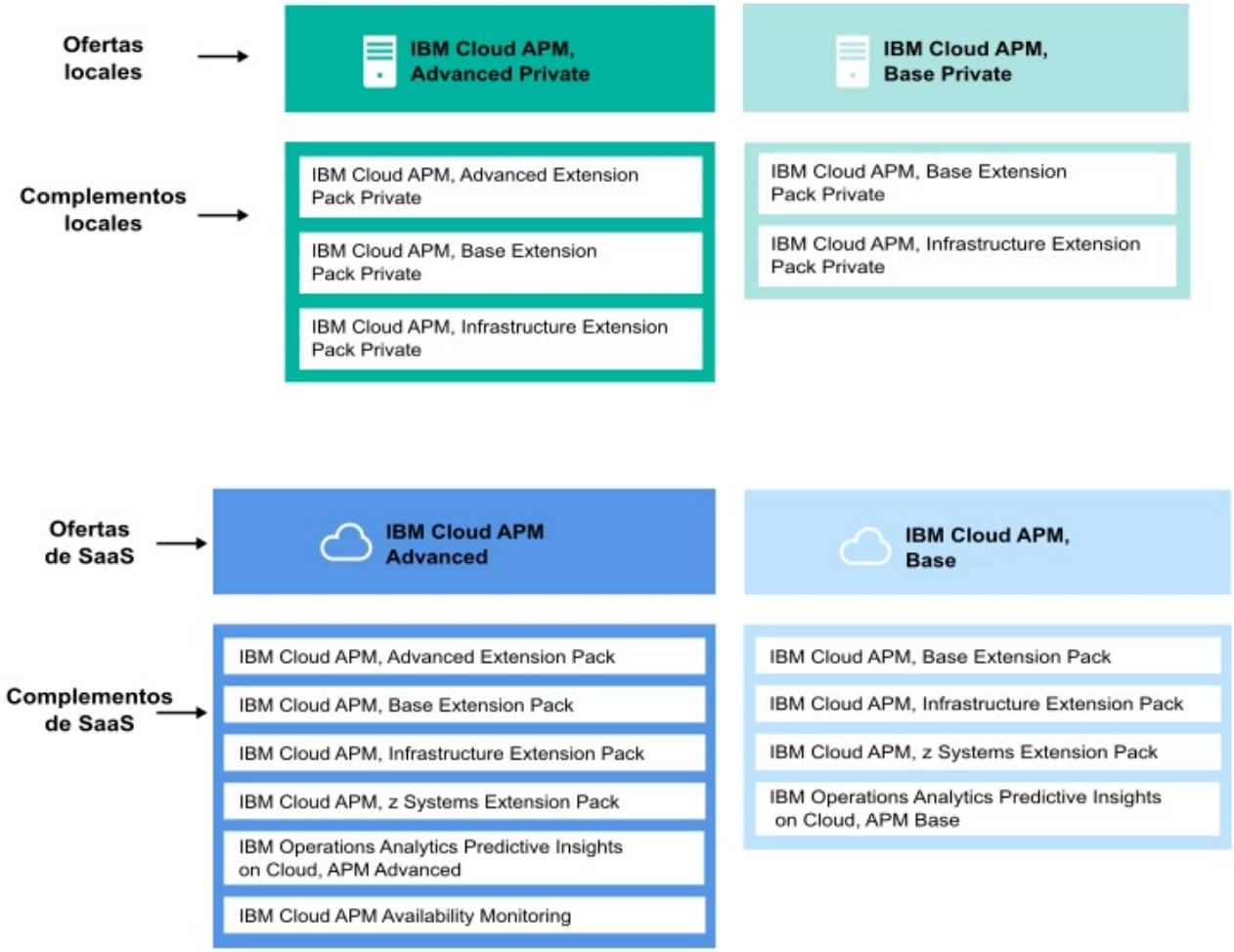
IBM Cloud Application Performance Management contiene dos ofertas y varios complementos. Las ofertas y los complementos contienen agentes y recopiladores de datos. Pueden utilizarse complementos específicos con cada oferta.

Para ver qué agentes están incluidos en una oferta o complemento y las prestaciones de agente y recopilador de datos, consulte “Capacidades” en la página 54.

Para cada oferta, hay complementos disponibles en IBM Marketplace. IBM Cloud Application Performance Management, Advanced es la oferta más amplia, la que incluye todos los agentes,

recopiladores de datos y páginas de panel de instrumentos. IBM Cloud Application Performance Management, Base es un subconjunto de Cloud APM, Advanced. Puede sustituir Cloud APM, Base por Cloud APM, Advanced en cualquier momento. La oferta final instalada después de esta sustitución será Cloud APM, Advanced. El diagrama muestra los complementos que están disponibles para cada oferta.

Los complementos son los mismos para todas las ofertas, salvo para Availability Monitoring, que es un complemento solo para la oferta Cloud APM, Advanced.



Ofertas

IBM Cloud Application Performance Management, Advanced

Esta oferta es para la experiencia del usuario final, el rastreo de transacciones y la supervisión de recursos de todos los componentes de la aplicación. Tiene visibilidad del nivel de código en las aplicaciones y el estado de los servidores de aplicaciones. Utilice el panel de instrumentos de diagnóstico para encontrar cuellos de botella de rendimiento en el código de aplicación y gestionar las aplicaciones críticas en producción.

La oferta incluye IBM Cloud Application Performance Management, Base y contiene agentes y recopiladores de datos que puede utilizar para supervisar las aplicaciones, transacciones y otros recursos instalados en la empresa. Para obtener una lista de los agentes y recopiladores de datos en esta oferta, consulte “Capacidades” en la página 54.

Con esta oferta, DevOps tiene una solución completa que proporciona visibilidad y control completos sobre las aplicaciones y la infraestructura. Los propietarios de línea de negocio pueden gestionar aplicaciones críticas y la experiencia del usuario final en producción. Los desarrolladores de aplicaciones pueden visualizar los detalles de las transacciones y diagnosticar los problemas de las aplicaciones.

IBM Cloud Application Performance Management, Base

Esta oferta es para la supervisión de recursos de infraestructura, los componentes de la aplicación y las cargas de trabajo en la nube. La supervisión de recursos ayuda a identificar y solucionar las transacciones lentas, los problemas de capacidad y las paradas. La oferta contiene agentes y recopiladores de datos que puede utilizar para supervisar las aplicaciones y otros recursos instalados en la empresa. Para obtener una lista de los agentes y recopiladores de datos en esta oferta, consulte "Capacidades" en la página 54.

Con esta oferta, los operadores de TI pueden solucionar las transacciones lentas, los problemas de capacidad y las paradas.

Complementos

Advanced Extension Pack

Este paquete de ampliación contiene el Monitoring Agent for SAP HANA Database, el Agente de SAP NetWeaver Java Stack y el Monitoring Agent for RabbitMQ.

Utilice el Agente de SAP HANA Database para supervisar la base de datos SAP HANA. Utilice el Agente de SAP NetWeaver Java Stack para supervisar la pila Java de SAP NetWeaver. Utilice el Agente de RabbitMQ para supervisar la mensajería de RabbitMQ. Este paquete de ampliación está disponible si tiene la oferta IBM Cloud Application Performance Management, Advanced.

Base Extension Pack

Este paquete de extensiones contiene los siguientes agentes:

- Monitoring Agent for Cassandra
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for Hadoop
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway

Utilice estos agentes para monitorizar una base de datos Cassandra, clúster Hadoop, recursos de servidor DataStage, aplicacionesMicrosoft Office 365, servidores Connect Direct y la aplicación Sterling File Gateway. Este paquete de ampliación está disponible si tiene una de las ofertas Cloud APM.

Infrastructure Extension Pack

Este paquete de extensiones contiene los siguientes agentes:

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for IBM Cloud

Utilice el Agente de Amazon EC2 para supervisar las instancias de Amazon EC2. Utilice el Agente de Amazon ELB para supervisar los Equilibradores de carga elásticos de AWS. Utilice el Agente de Azure Compute para supervisar las máquina virtuales de Azure Compute. Utilice Agente de Citrix VDI para supervisar la infraestructura de escritorio virtual Citrix.

Este paquete de ampliación está disponible si tiene una de las ofertas Cloud APM.

z Systems Extension Pack

Puede utilizar z Systems Extension Pack para visualizar los sucesos y datos de supervisión para los componentes de la aplicación OMEGAMON en la Consola de Cloud APM. Este paquete de ampliación está disponible si tiene una de las ofertas Cloud APM.

Operations Analytics - Predictive Insights

Este complemento es para analizar los datos de medida recopilados por Cloud APM y generar alarmas cuando se detectan anomalías. El complemento está disponible si tiene una de las ofertas Cloud APM.

Availability Monitoring
Este complemento es para la supervisión de la disponibilidad y el rendimiento de las aplicaciones web desde varios puntos de presencia distribuidos geográficamente. Este complemento no funciona como una oferta autónoma, pero está disponible si tiene la oferta IBM Cloud Application Performance Management, Advanced.

Si desea una visión general de las características en cada oferta, consulte "Detalles de las ofertas" en la página 50.

Para obtener una descripción de cada agente y recopilador de datos y enlaces a información específica de cada uno de ellos, consulte "Descripciones" en la página 58.

Detalles de las ofertas

Algunas características están disponibles para todas las ofertas y otras solamente lo están para determinadas ofertas.

Tabla 1 en la página 50 muestra características clave que están disponibles para cada oferta a simple vista.

Tabla 1. Características de cada oferta

Característica	Cloud APM, Advanced (Para DevOps, Desarrolladores y Línea de negocio)	Cloud APM, Base (Para Operaciones)
Supervisión de recursos de aplicación: Idiomas, middleware (la cobertura varía según la oferta).	✓	✓
Supervisión de sistema operativo: sistemas Linux, UNIX, Windows	✓	✓
Supervisión de archivos de registro: Utilice agentes de sistema operativo para supervisar archivos de registro de aplicación.	✓	✓
Paneles de instrumentos: • Consulte Tivoli Monitoring y los ICR de Cloud APM en los mismos paneles de instrumentos • Medidas históricas • Paneles de instrumentos personalizables	✓	✓
Interfaces API: Gestione su entorno utilizando las API.	✓	✓
Control de accesos basado en roles: Gestione el acceso y el privilegio de sus usuarios de IBM Cloud Application Performance Management.	✓	✓
Informes históricos: Genere informes para el rendimiento y el tiempo de respuesta de las aplicaciones que se han desglosado por transacción, dispositivo, navegador y otros (la cobertura varía en función de la oferta).	✓	✓
IBM Agent Builder: Cree agentes personalizados para supervisar cualquier plataforma o tecnología.	✓	✓

Tabla 1. Características de cada oferta (continuación)

Característica	Cloud APM, Advanced (Para DevOps, Desarrolladores y Línea de negocio)	Cloud APM, Base (Para Operaciones)
Supervisión de recursos de base de datos: (la cobertura varía en función de la oferta)	✓	✓
Supervisión de recursos de infraestructura: Hipervisores, almacenamiento y red (la cobertura varía en función de la oferta).	✓	✓
Supervisión de recursos de aplicaciones comerciales: Aplicaciones empresariales y de colaboración (la cobertura varía en función de la oferta).	✓	✓
Supervisión de tiempo de respuesta: Vea como el rendimiento de la aplicación afecta a los usuarios.	✓	✓
Integración con análisis de búsqueda: Busque la información para aislar, diagnosticar y resolver problemas rápidamente.	✓	✓
Operations Analytics - Predictive Insights (complemento): Determine las anomalías de rendimiento de la aplicación antes de que afecten a los usuarios.	✓	✓
Supervisión de la experiencia de usuario final real: Vea lo que experimentan los usuarios de su infraestructura en sus dispositivos.	✓	–
Rastreo de transacciones: Rastree las transacciones de extremo a extremo a través de su entorno de aplicación. • Topología de aplicación: Consulte cómo están conectados todos los componentes en el entorno de la aplicación. • Topología de instancia de transacción: Consulte la vía de acceso que se sigue a través del entorno para cada instancia de una transacción.	✓	–
Diagnósticos en profundidad: • Desglose los paneles de instrumentos de resumen hasta ver el nivel de código, el rastreo de pila y el detalle de consulta SQL para agentes específicos. • Detecte, diagnostique y termine las transacciones colgadas o lentas que aún estén en curso.	✓	–
Umbrales: Detecte comportamientos y condiciones de una aplicación específica basándose en definiciones supervisadas de forma activa.	✓	✓
Grupo de recursos: Categorice los sistemas gestionados de la empresa supervisada en función de su objetivo.	✓	✓

Están disponibles características adicionales como las siguientes para todas las ofertas a través de la integración con otros productos y componentes. Consulte “Integración ” en la página 82 y, para obtener más detalles, consulte Capítulo 8, “Integración con otros productos y componentes”, en la página 983).

- Agentes de Tivoli Monitoring y OMEGAMON: utilice la pasarela híbrida para recuperar datos y sucesos de supervisión para que esta información se visualice en la Consola de Cloud APM.
- Coexistencia de agentes: Instale agentes de Cloud APM en el mismo sistema donde están instalados agentes Tivoli Monitoring.
- Netcool/OMNIbus y otros receptores EIF: reenvío de sucesos a IBM Tivoli Netcool/OMNIbus.
- Alert Notification: reciba una notificación cuando el rendimiento de la aplicación exceda umbrales.
- IBM Control Desk: abra automáticamente tíquets en Control Desk.
- IBM Cloud: Supervisar aplicaciones IBM Cloud.

Agentes y recopiladores de datos

Los agentes y recopiladores de datos de IBM Cloud Application Performance Management están disponibles tanto en las ofertas como en los complementos.

Los agentes pueden supervisar muchos recursos de su entorno. Los recopiladores de datos pueden supervisar algunos recursos de IBM Cloud y locales. Existen los agentes correspondientes para todos los recopiladores de datos, excepto los recopiladores de datos de J2SE y de Python. Para obtener una lista de agentes y de recopiladores de datos y sus descripciones, consulte “Descripciones” en la página 58. Para averiguar las prestaciones que puede proporcionar el agente o el recopilador de datos en cada oferta, consulte “Capacidades” en la página 54. Para averiguar el historial de cambios de cada agente y recopilador de datos, consulte “Historial de cambios” en la página 52.

Puede instalar estos agentes o recopiladores de datos en función de su entorno y sus requisitos. Los recopiladores de datos envían datos directamente al Servidor de Cloud APM. Cuando se configura un agente, los recopiladores de datos envían datos al agente, que los reenvía al servidor. Los recopiladores de datos funcionan dentro del espacio de proceso de aplicaciones, mientras que los agentes se ejecutan como un proceso aparte fuera del espacio de proceso de aplicaciones.

Instale recopiladores de datos en las situaciones siguientes:

- Desea un proceso de instalación más sencillo.
- Utiliza contenedores.

Instale agentes en las situaciones siguientes:

- Desea una mayor escalabilidad.
- Desea limitar sockets de puntos finales al servidor.
- Cuando añade un umbral en el editor de umbrales, desea tener una lista despejada, que contenga solo los atributos del entorno que desea supervisar. Si utiliza un recopilador de datos, debe elegir entre los atributos de varios recopiladores de datos.
- Desea activar o desactivar algunas de las funciones de recopilación de datos en la IU, como por ejemplo los diagnósticos, el rastreo de transacciones o el rastreo de métodos.
- Desea ver datos de diagnósticos bajo demanda, como por ejemplo las solicitudes en curso y el vuelco de almacenamiento dinámico en el momento actual.

Historial de cambios

Descubra la información sobre las versiones y el historial de cambios de cada agente y recopilador de datos.

La siguiente tabla enumera los nombres de los agentes y recopiladores de datos con enlaces de notas técnicas del historial de cambios. Pulse los enlaces para ver los detalles del historial de cambios.

Tabla 2. Historial de cambios de agentes y recopiladores de datos	
Agentes y recopiladores de datos	**Enlaces**
Agente de Amazon EC2	Historial de cambios
Agente de Amazon ELB	Historial de cambios
Agente de Azure Compute	Historial de cambios
Agente de Cassandra	Historial de cambios
Agente de Cisco UCS	Historial de cambios
Agente de Citrix VDI	Historial de cambios
Agente de DataPower	Historial de cambios
Agente de DataStage	Historial de cambios
Agente de Db2	Historial de cambios
Agente de Hadoop	Historial de cambios
Agente de HMC Base	Historial de cambios
Agente de HTTP Server	Historial de cambios
Agente de IBM Cloud	Historial de cambios
Agente de IBM Integration Bus	Historial de cambios
Internet Service Monitoring	Historial de cambios
Recopilador de datos de J2SE	Historial de cambios
Agente de JBoss	Historial de cambios
Recopilador de datos de Liberty	Historial de cambios
Agente de Linux KVM	Historial de cambios
Agente de sistema operativo Linux	Historial de cambios
Agente de MariaDB	Historial de cambios
Agente de Microsoft Active Directory	Historial de cambios
Agente de Microsoft Cluster Server	Historial de cambios
Agente de Microsoft Exchange Server	Historial de cambios
Agente de Microsoft Hyper-V Server	Historial de cambios
Agente de Microsoft IIS	Historial de cambios
Agente de Microsoft .NET	Historial de cambios
Agente de Microsoft Office 365	Historial de cambios
Agente de Microsoft SharePoint Server	Historial de cambios
Agente de Microsoft SQL Server	Historial de cambios
Agente de MongoDB	Historial de cambios
Agente de MQ Appliance	Historial de cambios
Agente de MySQL	Historial de cambios
Agente de NetApp Storage	Historial de cambios

Tabla 2. Historial de cambios de agentes y recopiladores de datos (continuación)	
Agentes y recopiladores de datos	**Enlaces**
Agente de Node.js	Historial de cambios
Recopilador de datos de Node.js	Historial de cambios
Agente de OpenStack	Historial de cambios
Agente de Oracle Database	Historial de cambios
Agente de PHP	Historial de cambios
Agente de PostgreSQL	Historial de cambios
Recopilador de datos de Python	Historial de cambios
Agente de RabbitMQ	Historial de cambios
Agente de Supervisión de tiempo de respuesta	Historial de cambios
Agente de Ruby	Historial de cambios
Recopilador de datos de Ruby	Historial de cambios
Agente de SAP	Historial de cambios
Agente de SAP HANA Database	Historial de cambios
Agente de SAP NetWeaver Java Stack	Historial de cambios
Agente de Siebel	Historial de cambios
Agente de Skype for Business Server	Historial de cambios
Agente de Sterling Connect Direct	Historial de cambios
Agente de Sterling File Gateway	Historial de cambios
Agente de Sybase	Historial de cambios
Agente de Synthetic Playback	Historial de cambios
Agente de Tomcat	Historial de cambios
Agente de sistema operativo UNIX	Historial de cambios
Agente de VMware VI	Historial de cambios
Agente de WebLogic	Historial de cambios
Agente de WebSphere Applications	Historial de cambios
Agente de WebSphere Infrastructure Manager	Historial de cambios
Agente de WebSphere MQ	Historial de cambios
Agente de sistema operativo Windows	Historial de cambios

Capacidades

Las prestaciones de agente y recopilador de datos varían en función de la oferta. Las prestaciones clave de agente y recopilador de datos son la supervisión de recursos, el rastreo de transacciones y diagnósticos. Puede suscribirse a cualquiera de las ofertas y complementos de IBM Cloud Application Performance Management. Son necesarias ofertas específicas para complementos.

Cada agente y recopilador de datos supervisa los recursos que indica su nombre, por ejemplo Monitoring Agent for Cisco UCS supervisa los recursos de Cisco UCS.

En función de si usted es un desarrollador, en las operaciones, o propietario de una línea de negocio, puede utilizar prestaciones de Cloud APM diferentes.

- La prestación de supervisión de recursos incluye la supervisión de tiempo de respuesta, la supervisión de recursos de aplicación y la supervisión de recursos de infraestructura. Todos los agentes y recopiladores de datos pueden proporcionar la prestación de supervisión de recursos.
- La prestación de rastreo de transacciones proporciona información de topología e instancia de transacción.
- La prestación de diagnóstico incluye el rastreo y análisis de solicitudes individuales y, cuando es necesario, de llamadas a método.

Recuerde: La prestación de supervisión de recursos es común a todas las ofertas y complementos. Las prestaciones de rastreo de transacciones y diagnósticos solamente están disponibles en la oferta Cloud APM, Advanced y en los complementos.

Los agentes y recopiladores de datos para las aplicaciones que desea supervisar están disponibles para su descarga desde **Productos y servicios**. La instalación de los agentes tarda unos minutos. Los recopiladores de datos no requieren instalación y solamente puede configurarlos una vez finalizada la descarga. Para obtener instrucciones sobre la instalación de agentes, consulte Capítulo 6, “Instalación de los agentes”, en la página 125.

La Tabla 3 en la página 55 proporciona una lista exhaustiva de los agentes y recopiladores de datos, muestra qué oferta o complemento contiene el agente o recopilador de datos y muestra las prestaciones del agente o recopilador de datos. Cuando se indican complementos (por ejemplo, Infrastructure Extension Pack) para un agente o recopilador de datos, significa que son necesarios. Los agentes y los recopiladores de datos que dan soporte a las prestaciones de rastreo de transacciones y o diagnóstico también están anotados en la columna de Cloud APM, Advanced.

✓ indica que el agente o el recopilador de datos está disponible en la oferta y puede proporcionar la prestación de supervisión de recursos.

— indica que los datos o la prestación no está disponible en esta oferta o que el complemento no es necesario para el agente o el recopilador de datos.

TT indica rastreo de transacciones.

DD indica diagnóstico.

Tabla 3. Prestaciones de agente y recopilador de datos en cada oferta

Agentes y recopiladores de datos	Cloud APM, BaseCloud APM, Base Private	Cloud APM, Advanced	Complemento (si es necesario)
Agente de Amazon EC2	✓	✓	Infrastructure Extension Pack
Agente de Amazon ELB	✓	✓	Infrastructure Extension Pack
Agente de Azure Compute	✓	✓	Infrastructure Extension Pack
Agente de Cassandra	✓	✓	Base Extension Pack
Agente de Cisco UCS	✓	✓	—
Agente de Citrix VDI	✓	✓	Infrastructure Extension Pack

Tabla 3. Prestaciones de agente y recopilador de datos en cada oferta (continuación)

Agentes y recopiladores de datos	Cloud APM, BaseCloud APM, Base Private	Cloud APM, Advanced	Complemento (si es necesario)
Agente de Db2	✓	✓	—
Agente de DataPower	✓	✓ TT	—
Agente de DataStage	✓	✓	Base Extension Pack
Agente de Hadoop	✓	✓	Base Extension Pack
Agente de HMC Base	✓	✓	—
Agente de HTTP Server	✓	✓ TT	—
Agente de IBM Cloud	✓	✓	Infrastructure Extension Pack
Agente de IBM Integration Bus	—	✓ TT	—
Internet Service Monitoring	—	—	Base Extension Pack
Recopilador de datos de J2SE para aplicaciones locales	—	✓ TT DD	—
Agente de JBoss	✓	✓ TT DD	—
Recopilador de datos de Liberty para aplicaciones locales e IBM Cloud	—	✓ TT DD	—
Agente de Linux KVM	✓	✓	—
Agente de sistema operativo Linux	✓	✓	—
Agente de Microsoft Active Directory	✓	✓	—
Agente de Microsoft Cluster Server	✓	✓	—
Agente de Microsoft Exchange Server	✓	✓	—
Agente de Microsoft Hyper-V Server	✓	✓	—
Agente de Microsoft IIS	✓	✓	—

Tabla 3. Prestaciones de agente y recopilador de datos en cada oferta (continuación)

Agentes y recopiladores de datos	Cloud APM, BaseCloud APM, Base Private	Cloud APM, Advanced	Complemento (si es necesario)
Agente de Microsoft .NET	✓	✓ TT DD	—
Agente de Microsoft Office 365	✓	✓	Base Extension Pack
Agente de Microsoft SharePoint Server	✓	✓	—
Agente de Microsoft SQL Server	✓	✓	—
Agente de MongoDB	✓	✓	—
Agente de MQ Appliance	—	✓	—
Agente de MySQL	✓	✓	—
Agente de NetApp Storage	✓	✓	—
Agente de Node.js	✓	✓ DD	—
Recopilador de datos de Node.js para aplicaciones locales e IBM Cloud	—	✓ TT DD	—
Agente de OpenStack	✓	✓	—
Agente de Oracle Database	✓	✓	—
Agente de PHP	✓	✓	—
Agente de PostgreSQL	✓	✓	—
Recopilador de datos de Python para aplicaciones locales e IBM Cloud	✓	✓ DD	—
Agente de RabbitMQ	—	✓	Advanced Extension Pack
Agente de Supervisión de tiempo de respuesta	✓	✓ TT	—
Agente de Ruby	✓	✓ DD	—
Recopilador de datos de Ruby para aplicaciones IBM Cloud	—	✓ DD	—
Agente de SAP	—	✓	—
Agente de SAP HANA Database	—	✓	Advanced Extension Pack

Tabla 3. Prestaciones de agente y recopilador de datos en cada oferta (continuación)			
Agentes y recopiladores de datos	**Cloud APM, BaseCloud APM, Base Private**	**Cloud APM, Advanced**	**Complemento (si es necesario)**
Agente de SAP NetWeaver Java Stack	—	✓ TT DD	Advanced Extension Pack
Agente de Siebel	✓	✓	—
Agente de Skype for Business Server (anteriormente conocido como agente de Microsoft Lync Server)	✓	✓	—
Agente de Sterling Connect Direct	✓	✓	Base Extension Pack
Agente de Sterling File Gateway	✓	✓	Base Extension Pack
Agente de Sybase	✓	✓	—
Agente de Tomcat	✓	✓ TT	—
Agente de sistema operativo UNIX	✓	✓	—
Agente de VMware VI	✓	✓	—
Agente de WebLogic	✓	✓ TT DD	—
Agente de WebSphere Applications	✓	✓ TT DD	—
Agente de WebSphere Infrastructure Manager	✓	✓	—
Agente de WebSphere MQ	—	✓ TT	—
Agente de sistema operativo Windows	✓	✓	—

Para obtener más información sobre si el rastreo de transacciones o los diagnósticos se han habilitado de forma predeterminada para el agente o el recopilador de datos, consulte la tabla Habilitación del rastreo de transacciones para agentes y recopiladores de datos. Para obtener más información sobre paneles de instrumentos de diagnósticos predefinidos, consulte Paneles de instrumentos de diagnósticos de agentes y recopiladores de datos.

Descripciones

Las descripciones de los agentes y los recopiladores de datos proporcionan información sobre lo que cada uno de estos componentes supervisa y enlaces a más información sobre cada componente.

Cada agente y recopilador de datos tiene un número de versión, que cambia cada vez que se actualiza el agente o recopilador de datos. En cualquier release, se podrían añadir nuevos agentes o recopiladores de datos y actualizar los existentes. Si no tiene la última versión de un agente o recopilador de datos,

considere la posibilidad de actualizarlo. Si desea información sobre cómo comprobar la versión de un agente o recopilador de datos de su entorno, consulte Mandato de versión de agente.

Cada descripción de agente y recopilador de datos contienen enlaces a los tipos de detalles siguientes sobre esos componentes:

- Configuración de agente o recopilador de datos y otra información sobre prestaciones específicas del agente o recopilador de datos
- PDF de referencia que contiene descripciones de los paneles de instrumentos de agente o recopilador de datos de Cloud APM, widgets de grupo, umbrales, conjuntos de datos y atributos (métricas e ICR).

Para obtener enlaces a la documentación de agentes de IBM Tivoli Monitoring V6 y V7 que pueden coexistir con agentes y recopiladores de datos de Cloud APM V8, consulte Tabla 236 en la página 985.

Supervisión de Amazon EC2

Monitoring Agent for Amazon EC2 le proporciona un punto central de supervisión del estado, disponibilidad y rendimiento de las instancias de Amazon Elastic Compute Cloud (EC2). El agente muestra un conjunto integral de métricas para ayudarle a tomar decisiones informadas sobre su entorno de EC2, incluyendo el uso de CPU, uso de Elastic Block Store (EBS), uso de red, actualizaciones de mantenimiento de Amazon Web Services (AWS) y rendimiento de disco.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte “Configuración de la supervisión de Amazon EC2” en la página 197.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Amazon EC2 Reference (Referencia del agente de Amazon EC2).

Supervisión del Equilibrador de carga elástico de AWS

El Agente de Amazon ELB proporciona un punto central de supervisión del estado, la disponibilidad y el rendimiento de los Equilibradores de carga elásticos de AWS. El agente muestra un conjunto exhaustivo de métricas para cada aplicación de tipo equilibrador de carga, ayuda de red y clásica para ayudarle a tomar decisiones sobre su entorno de Equilibrador de carga elástico de AWS basadas en información.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte “Configuración de la supervisión del Equilibrador de carga elástico de AWS” en la página 205.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Amazon ELB Reference (Referencia del agente de Amazon ELB).

Supervisión de Azure Compute

El Agente de Azure Compute proporciona un punto central de supervisión del estado, la disponibilidad y el rendimiento de las instancias de Azure Compute. El agente muestra un conjunto de métricas integral para ayudarle a tomar decisiones informadas sobre el entorno de Azure Compute. Estas métricas incluyen el uso de CPU, el uso de red y el rendimiento de disco.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte “Configuración de la supervisión de Azure Compute” en la página 210.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Azure Compute Reference (Referencia del agente de Azure Compute).

Supervisión de Cassandra

El Monitoring Agent for Cassandra proporciona la posibilidad de supervisar el clúster de Cassandra. Puede recopilar y analizar información sobre los nodos, espacios de claves y familias de columnas del clúster de Cassandra.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte “Configuración de la supervisión de Cassandra” en la página 220.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de CassandraReference (referencia del agente de Cassandra).

Supervisión de Cisco UCS

Monitoring Agent for Cisco UCS proporciona un entorno para supervisar el estado, la red y el rendimiento de Cisco UCS. El agente de Cisco UCS proporciona una forma exhaustiva de recopilar y

analizar información específica de Cisco UCS necesaria para detectar los problemas con antelación y evitarlos.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Cisco UCS" en la página 223.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Cisco UCSReference (Referencia del agente de Cisco UCS).

Supervisión de Citrix Virtual Desktop Infrastructure

Monitoring Agent for Citrix Virtual Desktop Infrastructure le proporciona un punto central de supervisión del estado, disponibilidad y rendimiento de la infraestructura de escritorio virtual Citrix. El agente muestra un conjunto completo de métricas para ayudarle a tomar decisiones informadas sobre los recursos de XenDesktop o XenApp, incluyendo sitios, máquinas, aplicaciones, escritorios, sesiones, usuarios y más.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Citrix Virtual Desktop Infrastructure" en la página 230.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Citrix VDIReference (Referencia del agente de Citrix VDI).

Supervisión de DataPower

Monitoring Agent for DataPower proporciona un punto central de supervisión para Dispositivos DataPower en su entorno de empresa. Puede identificar y recibir notificaciones sobre problemas comunes con los dispositivos. El agente también proporciona información sobre rendimiento, recursos y carga de trabajo de los dispositivos.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración del Agente de DataPower " en la página 248.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte DataPower agent Reference (Referencia del agente de DataPower).
- Para obtener información sobre la supervisión de dispositivos DataPower como parte de la Pila de integración de IBM, consulte "Supervisión de la Pila de integración de IBM" en la página 101.

Supervisión de Db2

El Monitoring Agent for Db2 ofrece un punto central de supervisión de su entorno Db2. Puede supervisar un gran número de servidores desde una única consola de IBM Performance Management, con cada servidor supervisado por un agente de Db2. Puede recopilar y analizar información en relación con las aplicaciones, las bases de datos y los recursos del sistema.

- Para obtener información antes de actualizar a una nueva versión del agente, consulte "Agentes en AIX: Detención del agente y ejecución de slibclean antes de actualizar" en la página 1176
- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Db2 " en la página 252.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Db2Reference (Referencia del agente de Db2).
- Para obtener información sobre la supervisión de transacciones de base de datos como parte de la Pila de aplicaciones Java de IBM, consulte "Supervisión de la Pila de aplicaciones Java de IBM" en la página 94.

Supervisión de Hadoop

Monitoring Agent for Hadoop proporciona capacidades para supervisar el clúster Hadoop en la organización. Puede utilizar el agente para recopilar y analizar la información sobre el clúster Hadoop, como el estado de los nodos de datos y la máquina virtual Java, información de almacenamiento dinámico y no dinámico de memoria, e información sobre nodos Hadoop, sistemas de archivo y colas.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Hadoop" en la página 263.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de HadoopReference (Referencia del agente de Hadoop).

Supervisión de HMC Base

Monitoring Agent for HMC Base proporciona la capacidad de supervisar la consola de gestión de hardware (HMC). El agente supervisa la disponibilidad y el estado de los recursos de HMC: CPU, memoria, almacenamiento y red. El agente también informa del inventario de HMC y la configuración de servidores Power, agrupaciones de CPU y LPARs. La utilización de CPU de los servidores Power, las LPARs y las agrupaciones se supervisa mediante los datos de muestra de rendimiento de la HMC.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de HMC Base" en la página 273.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de HMC BaseReference (Referencia del agente de HMC Base).

Supervisión de HTTP Server

Monitoring Agent for HTTP Server recopila datos de rendimiento sobre IBM HTTP Server. Por ejemplo, se muestra información del servidor como puede ser el estado y el tipo del servidor, el número de errores de servidor y el número de inicios de sesión en el servidor satisfactorios y fallidos. Un recopilador de datos recopila los datos enviados al agente del servidor HTTP. El agente se ejecuta en el mismo sistema, con el servidor IBM HTTP Server que supervisa. Cada servidor supervisado está registrado como un subnodo. El módulo Tiempo de respuesta HTTP de IBM se instala con el agente de HTTP Server. Cuando se utiliza el agente de HTTP Server con el agente de Supervisión de tiempo de respuesta, el agente de WebSphere Application y un agente de base de datos, puede ver información de supervisión de transacciones desde el navegador en la base de datos para la pila de aplicaciones de IBM Java.

- Antes de empezar la instalación del agente, consulte Preinstalación en sistemas AIX - Agente de HTTP Server y Preinstalación en sistemas Linux - Agente de HTTP Server.
- Para obtener instrucciones sobre cómo revisar los valores del recopilador de datos y activar el recopilador de datos después de la instalación del agente, consulte "Configuración de la supervisión de HTTP Server" en la página 278.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de HTTP ServerReference (Referencia del agente de HTTP Server).
- Para obtener información sobre la supervisión de transacciones de servidor HTTP como parte de la Pila de aplicaciones Java de IBM, consulte "Supervisión de la Pila de aplicaciones Java de IBM" en la página 94.

Supervisión de IBM Cloud

Monitoring Agent for IBM Cloud recopila inventario de máquina virtual y métricas de la cuenta IBM Cloud (Softlayer). Utilice el agente de IBM Cloud para realizar el seguimiento de cuántos dispositivos virtuales se han configurado y se están ejecutando en IBM Cloud. Puede ver qué recursos se asignan a cada dispositivo virtual en la página del panel de instrumentos detallada, que también muestra información como el centro de datos en el que se encuentra un dispositivo, el sistema operativo y el ancho de banda de red público proyectado para el mes.

- Para obtener información sobre la configuración del agente después de la instalación, consulte Configuración de la supervisión de IBM Cloud.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de IBM CloudReference (Referencia del agente de IBM Cloud).

Supervisión de IBM Integration Bus

Monitoring Agent for IBM Integration Bus es una herramienta de supervisión y gestión que proporciona el medio de verificar, analizar y ajustar las topologías del intermediario de mensajes asociadas a los productos IBM WebSphere Message Broker e IBM Integration Bus.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de IBM Integration Bus" en la página 286.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de IBM Integration Bus Reference (Referencia del agente de IBM Integration Bus).

- Para obtener información sobre la supervisión de intermediarios de IBM Integration Bus como parte de la Pila de integración de IBM, consulte "Supervisión de la Pila de integración de IBM" en la página 101.

Supervisión de InfoSphere DataStage

El agente de supervisión de InfoSphere DataStage supervisa la disponibilidad, el uso de recursos y el rendimiento del servidor DataStage. El agente supervisa el estado de salud de los trabajos y nodos del motor. Puede analizar la información que el agente recopila y realizar las acciones adecuadas para resolver problemas en el servidor DataStage.

- Para obtener información sobre la configuración del agente después de la instalación, consulte Configuración de la supervisión de InfoSphere DataStage.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de DataStage Reference (Referencia del agente de DataStage).

Internet Service Monitoring

Internet Service Monitoring permite determinar si un servicio determinado tiene el rendimiento adecuado, identificar áreas problemáticas e informar sobre el rendimiento del servicio en relación con los acuerdos de nivel de servicio. Agente de Internet Service Monitoring funciona emulando las acciones de un usuario real. Sondea o prueba periódicamente los servicios de Internet para comprobar su estado y rendimiento.

- Para obtener información sobre cómo configurar el agente tras la instalación, consulte "Configuración del agente en sistemas Windows " en la página 464
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Internet Service Monitoring Agent Reference (Referencia del agente de Internet Service Monitoring).

Supervisión del recopilador de datos de J2SE

El recopilador de datos de J2SE recopila datos de diagnóstico detallado y supervisión de recursos para aplicaciones Java. Los datos de diagnóstico detallado se muestran en los paneles de instrumentos en función de las solicitudes y la información agregada para dar soporte a varias vistas con mayor nivel de detalle. Tanto la supervisión de recursos como los diagnósticos en profundidad están soportados, lo que ayuda a detectar, aislar y diagnosticar problemas de las aplicaciones Java. Puede configurar el recopilador de datos para diagnosticar solicitudes lentas.

- Para obtener información sobre la configuración del recopilador de datos, consulte Configuración del recopilador de datos de J2SE.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte J2SE data collector Reference (Referencia del recopilador de datos de J2SE).

Supervisión de JBoss

Monitoring Agent for JBoss supervisa los recursos de los servidores de aplicaciones de JBoss y la plataforma JBoss Enterprise Application. Utilice los paneles de instrumentos proporcionados con el agente de JBoss para identificar las aplicaciones más lentas, las solicitudes más lentas, los cuellos de botella de agrupaciones de hebras, problemas de recogida de basura y memoria de almacenamiento dinámico de JVM, las sesiones más ocupadas y otros cuellos de botella del servidor de aplicaciones JBoss.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de JBoss" en la página 475.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de JBoss Reference (Referencia del agente de JBoss).

Supervisión de Linux KVM

El Monitoring Agent for Linux KVM es un agente multiinstancia y multiconexión, y da soporte a conexiones con el hipervisor KVM basado en Enterprise Linux y los entornos Red Hat Enterprise Virtualization Manager (RHEV-M). Puede crear varias instancias de este agente para supervisar varios hipervisores en un entorno de hipervisor de RHEV-M o KVM. Puede supervisar cargas de trabajo virtualizadas y analizar la capacidad de recursos entre varias máquinas virtuales. Para conectar el

agente a una máquina virtual en el entorno de hipervisor KVM, debe instalar los requisitos previos: `libvirt*.rpm` y Korn Shell Interpreter (pdksh). El agente recopila medidas conectando remotamente a un hipervisor libvirt que gestiona las máquinas virtuales.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Linux KVM" en la página 490.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Linux KVM Reference (Referencia del agente de Linux KVM).

Supervisión de SO Linux

Monitoring Agent for Linux OS proporciona capacidades de supervisión para la disponibilidad, el rendimiento y el uso de recursos del entorno del SO Linux. Este agente da soporte a la supervisión de contenedores de Docker. Por ejemplo, se muestra información detallada como el uso de CPU, memoria, red e información de uso de E/S relacionada con el contenedor de Docker. También se muestra la información general sobre los contenedores de Docker que se ejecutan en el servidor, como por ejemplo el ID de Docker y el nombre de instancia. Además, puede configurar la supervisión de archivos de registro para supervisar archivos de registro de aplicación. Puede recopilar y analizar información específica del servidor, como por ejemplo el rendimiento del sistema operativo y la CPU, información del disco Linux y análisis de rendimiento, análisis de estado de proceso y el rendimiento de la red.

- Para obtener información sobre la configuración de la supervisión de archivos de registro después de la instalación, consulte "Configuración de la supervisión de archivos de registro del agente de sistema operativo" en la página 656.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de sistema operativo Linux Reference (Referencia del agente de sistema operativo Linux).

Supervisión de MariaDB

Monitoring Agent for MariaDB ofrece un punto central de la gestión para la aplicación o el entorno de MariaDB. El software proporciona medios completos para recopilar la información necesaria para detectar problemas de forma precoz y evitarlos. La información está estandarizada en todo el sistema. Puede supervisar varios servidores desde una única consola. Mediante Monitoring Agent for MariaDB, puede recopilar y analizar fácilmente información específica de MariaDB.
Para obtener información sobre la configuración del agente después de la instalación, consulte "Configuración de la supervisión de MariaDB" en la página 502

Supervisión de Microsoft Active Directory

Monitoring Agent for Microsoft Active Directory proporciona capacidades para supervisar Active Directory en la organización. Puede utilizar el agente para recopilar y analizar información es específica de Active Directory, como por ejemplo el estado de la red, la réplica de Sysvol, el rendimiento de la libreta de direcciones, y el uso del sistema directorio.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Microsoft Active Directory" en la página 505.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Microsoft Active Directory Reference (Referencia del agente de Microsoft Active Directory).

Supervisión de Microsoft Cluster Server

Monitoring Agent for Microsoft Cluster Server proporciona prestaciones para supervisar Microsoft Cluster Server en su organización. Puede utilizar el agente de Microsoft Cluster Server para recopilar información relacionada con la disponibilidad de recursos, como por ejemplo el nivel de clúster, los nodos de clúster, los grupos de recursos de clúster, los recursos de clúster y las redes de clúster. El agente también proporciona estadísticas de uso de recursos de clúster, como por ejemplo el uso del procesador, el uso de la memoria, el uso del disco y el uso de la red.

- Para obtener información sobre la configuración del agente después de la instalación, consulte "Configuración de la supervisión de Microsoft Cluster Server" en la página 513.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Microsoft Cluster Server Reference (Referencia del agente de Microsoft Cluster Server).

Supervisión de Microsoft Exchange Server

Monitoring Agent for Microsoft Exchange Server proporciona capacidades para supervisar el estado, la disponibilidad y el rendimiento de los servidores Exchange Server de su organización. Puede utilizar el agente de Microsoft Exchange Server para recopilar información específica del servidor, como por ejemplo el correo electrónico, el estado de las base de datos de buzón y las actividades de los clientes. Además, el agente proporciona estadísticas del uso de memoria caché, uso de correo, uso de base de datos y actividades del cliente para facilitarle el análisis del rendimiento de Exchange Servers.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Microsoft Exchange" en la página 515.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Microsoft Exchange Server Reference (Referencia del agente de Microsoft Exchange Server).

Supervisión de Microsoft Hyper-V Server

Monitoring Agent for Microsoft Hyper-V Server proporciona la capacidad de supervisar la disponibilidad y el rendimiento de todos los sistemas Hyper-V de la organización. Agente de Microsoft Hyper-V Server proporciona información de configuración como por ejemplo el número de máquinas virtuales, el estado de las máquinas virtuales, el número de discos virtuales asignados, la memoria virtual asignada y el números de procesadores virtuales asignados. Además, el agente proporciona estadísticas del uso de procesadores físicos, del uso de memoria, del uso de red, del uso de procesadores lógicos y del uso de procesadores virtuales.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Microsoft Hyper-V" en la página 528.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Microsoft Hyper-V Server Reference (Referencia del agente de Microsoft Hyper-V Server).

Supervisión de Microsoft Internet Information Services

Monitoring Agent for Microsoft Internet Information Services proporciona la capacidad de supervisar la disponibilidad y el rendimiento de Microsoft Internet Information Server. Puede utilizar el agente de Microsoft Internet Information Server para supervisar los detalles del sitio web como por ejemplo la tasa de solicitudes, la tasa de transferencia de datos, las estadísticas de error y las estadísticas de conexiones.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Microsoft IIS" en la página 532.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Microsoft IIS Reference (Referencia del agente de Microsoft IIS).

Supervisión de Microsoft .NET

Monitoring Agent for Microsoft .NET supervisa aplicaciones de Microsoft .NET basadas en Internet Information Services (IIS) y recursos de Microsoft .NET Framework . El componente recopilador de datos recopila datos de solicitudes HTTP entrantes. El recopilador de datos recopila llamadas de método y construye un árbol de llamadas, y recopila datos de contexto de solicitud y rastreo de pila. Utilice los paneles de instrumentos que se proporcionan con el agente Microsoft .NET para identificar los problemas asociados con Microsoft .NET Framework y también para identificar las solicitudes HTTP más lentas desde las que puede acceder al detalle de la información de seguimiento de pila para aislar los problemas.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Registro del recopilador de datos" en la página 542.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Microsoft .NET Reference (Referencia del agente de Microsoft .NET).

Supervisión de Microsoft Office 365

El Monitoring Agent for Microsoft Office 365 proporciona la posibilidad de supervisar Microsoft Office 365. Puede recopilar y analizar información sobre Microsoft Exchange Online, SharePoint Online, Skype for Business y OneDrive for Business.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Microsoft Office 365" en la página 551.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Microsoft Office 365 Reference (Referencia del agente de Microsoft Office 365).

Supervisión de Microsoft SharePoint Server

Monitoring Agent for Microsoft SharePoint Server proporciona el entorno para supervisar la disponibilidad, los sucesos y el rendimiento de Microsoft SharePoint Server. Utilice este agente para recopilar datos de Microsoft SharePoint Server y gestionar operaciones.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Microsoft SharePoint Server " en la página 557.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Microsoft SharePoint Server Reference (Referencia del agente de Microsoft SharePoint Server).

Supervisión de Microsoft SQL Server

Monitoring Agent for Microsoft SQL Server proporciona la posibilidad de supervisar Microsoft SQL Server. El agente de Microsoft SQL Server ofrece un punto central de gestión de las bases de datos distribuidas. Utilice los paneles de instrumentos de agente de Microsoft SQL Server para supervisar la disponibilidad, el rendimiento, el uso de recursos y el estado general de todas las instancias de SQL Server que se están supervisando.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Microsoft SQL Server " en la página 560.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Microsoft SQL Server Reference (Referencia del agente de Microsoft SQL Server).

Supervisión de MongoDB

Monitoring Agent for MongoDB proporciona la capacidad de supervisión para el uso, el estado y el rendimiento del despliegue de MongoDB. Puede recopilar y analizar información como por ejemplo el uso de la capacidad de base de datos, el porcentaje de conexiones abiertas, el uso de la memoria, el estado de la instancia y el tiempo de respuesta en los paneles de instrumentos visualizados.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de MongoDB" en la página 593.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de MongoDB Reference (Referencia del agente de MongoDB).

Supervisión de MQ Appliances

Monitoring Agent for MQ Appliance proporciona información de supervisión que se centra en el nivel de dispositivo MQ en MQ Appliances, por ejemplo, información de memoria de CPU, memoria, almacenamiento, sensores y gestor de colas.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de IBM MQ Appliances" en la página 301.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte MQ Appliance agent Reference (Referencia del agente de MQ Appliance).

Supervisión de MySQL

Monitoring Agent for MySQL proporciona prestaciones de supervisión para el estado, el uso y el rendimiento del despliegue de MySQL. Puede recopilar y analizar información como por ejemplo Bytes recibidos y enviados, Páginas de agrupación de almacenamiento intermedio InnoDB y Rendimiento histórico.

- Antes de empezar la instalación del agente, consulte Preinstalación en sistemas Linux - Agente de MySQL o Preinstalación en sistemas Windows - Agente de MySQL.
- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de MySQL" en la página 599.

- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de MySQL Reference (Referencia del agente de MySQL).

Supervisión de Almacenamiento de NetApp

El Monitoring Agent for NetApp Storage proporciona la capacidad de supervisar los sistemas de almacenamiento de NetApp mediante el OCUM (OnCommand Unified Manager) de NetApp. Puede recopilar y analizar información acerca de los conjuntos, nodos, discos y volúmenes de los sistemas de almacenamiento de NetApp.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de NetApp Storage" en la página 602.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de NetApp Storage Reference (Referencia del agente de NetApp Storage).

Supervisión de Node.js

Monitoring Agent for Node.js o el recopilador de datos de Node.js autónomo puede utilizarse para medir y recopilar datos sobre el rendimiento de las aplicaciones Node.js. Por ejemplo, el rendimiento y los tiempos de respuesta de las solicitudes HTTP y otras mediciones relacionadas con el uso de recursos, se supervisan y se almacenan para visualización y análisis. Para elegir entre el Agente de Node.js y el Recopilador de datos de Node.js, consulte "Configuración de la supervisión de Node.js" en la página 608 para obtener instrucciones.

Agente de Node.js

- Antes de empezar la instalación, consulte Preinstalación en sistemas Linux - Agente de Node.js.
- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración del Agente de Node.js" en la página 609.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Node.js Reference (Referencia del agente de Node.js).

Recopilador de datos de Node.js (autónomo)

El Recopilador de datos de Node.js supervisa aplicaciones IBM Cloud y locales. La supervisión de recursos y los diagnósticos en profundidad están soportados, lo que ayuda a detectar, aislar y diagnosticar problemas de las aplicaciones. Puede configurar el recopilador de datos para hacer un seguimiento del rendimiento de llamadas de método y solicitudes individuales, y utilizar la información para diagnosticar solicitudes lentas y realizar acciones de acuerdo con ello.

Aplicaciones de IBM Cloud

- Para obtener información sobre la configuración del recopilador de datos, consulte "Configuración del Recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud (anteriormente Bluemix)" en la página 615.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Data collectors Reference (Referencia de recopiladores de datos).

Aplicaciones locales

- Para obtener información sobre la configuración del recopilador de datos, consulte "Configuración del Recopilador de datos de Node.js autónomo para aplicaciones locales" en la página 621.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Data collectors Reference (Referencia de recopiladores de datos).

Supervisión de OpenStack

Monitoring Agent for OpenStack proporciona prestaciones para supervisar las aplicaciones de OpenStack. Utilice los paneles de instrumentos para ver el rendimiento de las aplicaciones de OpenStack, como por ejemplo la información sobre puntos finales de API, conexión de servidor SSH, procesos e hipervisores.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración del Agente de OpenStack" en la página 633.

- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de OpenStack Reference (Referencia del agente de OpenStack).

Supervisión de base de datos de Oracle

El Monitoring Agent for Oracle Database proporciona prestaciones de supervisión para la disponibilidad, el rendimiento y el uso de recursos del entorno de base de datos Oracle. Puede configurar más de una instancia de Agente de Oracle Database para supervisar diferentes bases de datos de Oracle. Este agente también proporciona la capacidad de supervisión remota.

- Antes de empezar la instalación del agente, consulte Preinstalación en sistemas AIX - Agente de Oracle Database, Preinstalación en sistemas Linux - Agente de Oracle Database o Preinstalación en sistemas Windows - Agente de Oracle Database (Windows).
- Para obtener instrucciones sobre la configuración del agente después de la instalación, consulte "Configuración de la supervisión de base de datos de Oracle" en la página 638.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Oracle Database Reference (Referencia del agente de Oracle Database).
- Para obtener información sobre la supervisión de transacciones de base de datos como parte de la Pila de aplicaciones Java de IBM, consulte "Supervisión de la Pila de aplicaciones Java de IBM" en la página 94.

Supervisión de PHP

El Monitoring Agent for PHP supervisa aplicaciones web PHP recopilando medidas de acceso web a través de un servidor web Apache y datos de estadísticas de rendimiento de MySQL. El agente descubre todas las aplicaciones de WordPress en un servidor Apache y proporciona información de estadísticas de aplicación de WordPress. Utilice el agente de PHP para supervisar la disponibilidad del servidor web, el estado del servidor Apache y solicitudes GET/POST. El agente solo evalúa el rendimiento de las peticiones PHP en aplicaciones WordPress. No se evalúan las cargas de CSS y JS. El agente no utiliza argumentos de URL para identificar los URL.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de PHP" en la página 688.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de PHP Reference (Referencia del agente de PHP).

Supervisión de PostgreSQL

El Monitoring Agent for PostgreSQL supervisa la base de datos de PostgreSQL recopilando medidas de PostgreSQL a través de un controlador JDBC. El agente proporciona datos sobre el uso de recursos del sistema, la capacidad de la base de datos, las conexiones utilizadas, el estado individual de las instancias en ejecución, estadísticas de operaciones, el tiempo de respuesta de las sentencias de consulta SQL, detalles de tamaño de base de datos e información de bloqueo.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de PostgreSQL" en la página 690.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de PostgreSQL Reference (Referencia del agente de PostgreSQL).

Supervisión de Python

El recopilador de datos de Python supervisa tanto en aplicaciones locales como IBM Cloud Python. Tanto la supervisión de recursos como los diagnósticos en profundidad están soportados, lo que proporciona datos de supervisión como por ejemplo uso de CPU y memoria, recogida de basura y hebras. Puede configurar el recopilador de datos para hacer un seguimiento del rendimiento de llamadas de método y solicitudes individuales, y utilizar la información para diagnosticar solicitudes lentas y realizar acciones de acuerdo con ello.

Aplicaciones de IBM Cloud

- Para obtener información sobre la configuración del recopilador de datos, consulte "Configuración del recopilador de datos de Python para aplicaciones IBM Cloud" en la página 695.

- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Data collectors Reference.

Aplicaciones locales

- Para obtener información sobre la configuración del recopilador de datos, consulte "Configuración del Recopilador de datos de Python para aplicaciones locales" en la página 701.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Data Collector Reference.

Supervisión de RabbitMQ

El Monitoring Agent for RabbitMQ proporciona la posibilidad de supervisar el clúster de RabbitMQ. Puede recopilar y analizar información sobre los nodos, colas y canales del clúster de RabbitMQ.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de RabbitMQ " en la página 707.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de RabbitMQ Reference (Referencia del agente de RabbitMQ).

Supervisión de tiempo de respuesta

Agente de Supervisión de tiempo de respuesta utiliza la supervisión de red para capturar datos de transacciones HTTP y HTTPS como por ejemplo tiempos de respuesta y códigos de estado. Utilice el agente de Supervisión de tiempo de respuesta para supervisar el rendimiento y la disponibilidad de aplicaciones web para usuarios, incluyendo la información de solicitud de transacción, aplicación y servidor. Además, utilice este agente para supervisar dispositivos e información de sesión.

- Antes de empezar la instalación de Agente de Supervisión de tiempo de respuesta, consulte Preinstalación en sistemas AIX - Agente de Supervisión de tiempo de respuesta, Preinstalación en sistemas Linux - Agente de Supervisión de tiempo de respuesta o Preinstalación en sistemas Windows - Agente de Supervisión de tiempo de respuesta.
- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Inyección JavaScript" en la página 714.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Transaction Monitoring Reference (Referencia de supervisión de transacciones).
- Para obtener información sobre la supervisión de tiempo de respuesta como parte de la Pila de aplicaciones Java de IBM, consulte "Supervisión de la Pila de aplicaciones Java de IBM" en la página 94.

Supervisión de Ruby

Monitoring Agent for Ruby supervisa el rendimiento de las aplicaciones Ruby on Rails, incluyendo estadísticas de configuración y tráfico de solicitudes. También puede utilizar la función de diagnóstico para obtener una vista más profunda de cada aplicación.

El Recopilador de datos de Ruby autónomo supervisa solo aplicaciones IBM Cloud.

Agente de Ruby

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Ruby" en la página 743.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Ruby Reference (Referencia del agente de Ruby).

Recopilador de datos de Ruby (autónomo)

Puede utilizar el recopilador de datos de Ruby para supervisar aplicaciones IBM Cloud. Tanto la supervisión de recursos como los diagnósticos en profundidad están soportados, lo que ayuda a detectar, aislar y diagnosticar problemas de las aplicaciones. Puede configurar el recopilador de datos para hacer un seguimiento del rendimiento de llamadas de método y solicitudes individuales, y utilizar la información para diagnosticar solicitudes lentas y realizar acciones de acuerdo con ello.

Aplicaciones de IBM Cloud

- Para obtener información sobre la configuración del recopilador de datos, consulte Configuración del recopilador de datos de Ruby.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Data collectors Reference.

Supervisión de aplicaciones SAP

Monitoring Agent for SAP Applications proporciona la capacidad de supervisar las aplicaciones SAP que se ejecutan en la pila ABAP (Advanced Business Application Programming). El agente también supervisa SAP Solution Manager, que es una herramienta de gestión del ciclo de vida SAP, y SAP PI (SAP NetWeaver Process Integration), que es un software de integración de proceso para SAP. Ofrece un punto central de gestión para recopilar la información necesaria para detectar problemas con prontitud y para seguir los pasos necesarios para evitar que vuelvan a producirse. Permite la gestión eficaz de sistemas entre releases, aplicaciones y componentes SAP, y las bases de datos, los sistemas operativos y las interfaces externas subyacentes.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de SAP" en la página 756.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de SAP Reference (Referencia del agente de SAP).

Supervisión de base de datos SAP HANA

Monitoring Agent for SAP HANA Database supervisa la disponibilidad, el uso de recurso y el rendimiento de la base de datos SAP HANA. El agente puede supervisar casos de ejemplo de despliegue de HANA; por ejemplo, un solo host - una sola base de datos, un solo host - varias bases de datos de arrendatario, varios hosts – una sola base de datos y varios hosts – varias bases de datos de arrendatario. Puede analizar la información que el agente recopila y realizar las acciones adecuadas para resolver problemas en la base de datos SAP HANA.

- Antes de empezar la instalación del agente, consulte Preinstalación en sistemas AIX - Agente de SAP HANA Database o Preinstalación en sistemas Linux - Agente de SAP HANA Database o Preinstalación en sistemas Windows - Agente de SAP HANA Database.
- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de base de datos SAP HANA" en la página 789.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de SAP HANA Database Reference (Referencia del agente de base de datos SAP HANA).

Supervisión de SAP NetWeaver Java Stack

Monitoring Agent for SAP NetWeaver Java Stack supervisa la disponibilidad, el uso de recursos y el rendimiento de SAP NetWeaver Java Stack. El agente puede supervisar los escenarios del despliegue de la pila Java de SAP NetWeaver como, por ejemplo, un único host - una única instancia, un único host - varias instancias, varios hosts - varias instancias y varios hosts - varias instancias. Puede analizar la información que el agente recopila y realizar las acciones adecuadas para resolver problemas en la pila Java de SAP NetWeaver.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de SAP NetWeaver Java Stack" en la página 792.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de SAP NetWeaver Java Stack Reference (Referencia del agente de SAP NetWeaver Java Stack).

Supervisión de Siebel

Monitoring Agent for Siebel proporciona un punto central de supervisión de los recursos de Siebel, que incluyen estadísticas de Siebel, sesiones de usuario, componentes, tareas, servidor de la aplicaciones, Servidor de nombres de pasarela de Siebel, uso de memoria y CPU de proceso y supervisión de sucesos de registro.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Siebel" en la página 799.

- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Siebel Reference (Referencia del agente de Siebel).

Supervisión de Skype for Business Server (anteriormente conocido como Microsoft Lync Server)
El Monitoring Agent for Skype for Business Server le proporciona la capacidad de supervisar el estado, la disponibilidad y el rendimiento de Skype for Business Server. Puede utilizar el agente de Skype for Business Server para recopilar información específica del servidor como, por ejemplo, latencia, transacciones sintéticas, operaciones de grabación de servicio CDR (grabación de detalles de llamada), estado de solicitudes reguladas e iguales SIP (Session Initiation Protocol). Además, el agente proporciona estadísticas de uso histórico de mensajería instantánea y servidor de mediación para ayudarle a analizar el rendimiento de los servidores Lync o Skype for Business.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Skype for Business Server (anteriormente conocido como Microsoft Lync Server)" en la página 535.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Skype for Business Server Reference (Referencia del agente de Skype for Business Server).

Supervisión de Sterling Connect Direct
Monitoring Agent for Sterling Connect Direct proporciona la capacidad de supervisión de los servidores de Connect Direct. Proporciona información de estado y rendimiento de los servidores. Además, ofrece un análisis de la actividad de transferencia de archivos.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Sterling Connect Direct" en la página 811.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Sterling Connect Direct Reference (Referencia del agente de Sterling Connect Direct).

Supervisión de Sterling File Gateway
El Monitoring Agent for Sterling File Gateway supervisa la aplicación Sterling File Gateway, que se utiliza para transferir archivos entre socios internos y externos mediante distintos protocolos, distintas convenciones de nomenclatura y distintos formatos de archivo. También da soporte a la función de supervisión remota.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Sterling File Gateway" en la página 814.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Sterling File Gateway Reference (Referencia del agente de Sterling File Gateway).

Supervisión de Sybase Server
El Monitoring Agent for Sybase Server ofrece un punto central de gestión de las bases de datos distribuidas. Recopila la información necesaria para que los administradores del sistema y de la base de datos puedan examinar el rendimiento del sistema del servidor Sybase, detectar problemas y evitarlos.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión del servidor Sybase" en la página 821.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de SybaseReference (Referencia del agente de Sybase)..

Supervisión de Tomcat
Monitoring Agent for Tomcat supervisa los recursos de servidores de aplicaciones Tomcat. Utilice los paneles de instrumentos proporcionados con el agente de Tomcat para identificar las aplicaciones más lentas, las solicitudes más lentas, los cuellos de botella de agrupaciones de hebras, problemas de recogida de basura y memoria de almacenamiento dinámico de JVM, las sesiones más ocupadas y otros cuellos de botella del servidor de aplicaciones Tomcat.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de Tomcat" en la página 829.

- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de Tomcat Reference (Referencia del agente de Tomcat).

Supervisión de SO UNIX

Monitoring Agent for UNIX OS proporciona prestaciones de supervisión para la disponibilidad, el rendimiento y el uso de recursos del entorno de sistema operativo UNIX. (solo sistema operativo AIX y Solaris. Consulte Requisitos del sistema en APM Developer Center.) Además, puede configurar la supervisión de archivos de registro para supervisar archivos de registro de aplicación. Puede recopilar y analizar información específica del servidor, como por ejemplo el rendimiento del sistema operativo y la CPU, información del disco UNIX y análisis de rendimiento, análisis de estado de proceso y el rendimiento de la red.

- Para obtener información sobre la configuración de la supervisión de archivos de registro después de la instalación, consulte "Configuración de la supervisión de archivos de registro del agente de sistema operativo" en la página 656.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de sistema operativo UNIX Reference (Referencia del agente de sistema operativo UNIX).

Supervisión de VMware VI

Monitoring Agent for VMware VI supervisa la Infraestructura virtual de VMware mediante la conexión a VMware Virtual Center. Puede utilizar el agente de VMware VI para ver el resumen de estado para los clústeres y supervisar varios componentes como clústeres, máquinas virtuales, almacenes de datos y servidores ESX desde una sola consola.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de VMware VI" en la página 837.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de VMware VI Reference (Referencia del agente de VMware VI).

Supervisión de WebLogic

Monitoring Agent for WebLogic proporciona un punto central de supervisión del estado, disponibilidad y rendimiento del entorno de servidor WebLogic. El agente muestra un conjunto completo de métricas para ayudarle a tomar decisiones informadas sobre los recursos de WebLogic, incluyendo máquinas virtuales Java (JVM), Java Message Service (JMS) y Java Database Connectivity (JDBC).

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de WebLogic" en la página 846.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de WebLogic Reference (Referencia del agente de WebLogic).

Supervisión de WebSphere Applications

Monitoring Agent for WebSphere Applications con el recopilador de datos incorporado o el recopilador de datos de Liberty supervisan los recursos de los servidores de aplicaciones de WebSphere. Estos componentes de supervisión se pueden configurar para realizar lo siguiente:

- Recopilar medidas de PMI para la supervisión de recursos a través de una interfaz de JMX en el servidor de aplicaciones.
- Recopilar medidas de rendimiento de solicitud agregadas.
- Realizar el seguimiento del rendimiento de llamadas de método y solicitudes individuales.

Los datos de supervisión se visualizan en los paneles de instrumentos. Puede utilizar los paneles de instrumentos proporcionados para aislar áreas de problema específicas de su servidor de aplicaciones. Aumente el nivel de detalle para determinar si hay un problema dentro de un recurso subyacente o si está relacionado con el código de la aplicación.

Para obtener información sobre si desea utilizar el agente o uno de los recopiladores de datos, consulte "Configuración de la supervisión de WebSphere Applications" en la página 862.

Agente de WebSphere Applications y recopilador de datos incorporado

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración del recopilador de datos para Agente de WebSphere Applications" en la página 863.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de WebSphere Applications Reference (Referencia del agente de WebSphere Applications).
- Para obtener información sobre la supervisión de WebSphere Application Server como parte de la Pila de aplicaciones Java de IBM, consulte "Supervisión de la Pila de aplicaciones Java de IBM" en la página 94.

Recopilador de datos Liberty (autónomo)

Puede utilizar el recopilador de datos de Liberty para supervisar el perfil de WebSphere Liberty en IBM Cloud o para supervisar WebSphere Application Server Liberty on Linux for System x. La supervisión de recursos, los diagnósticos y el rastreo de transacciones están todos soportados, lo que ayuda a detectar, aislar y diagnosticar problemas de las aplicaciones. Puede configurar el recopilador de datos autónomo para hacer un seguimiento del rendimiento de llamadas de método y solicitudes individuales, y utilizar la información para diagnosticar solicitudes lentas y realizar acciones de acuerdo con ello.

Aplicaciones de IBM Cloud

- Para obtener información sobre la configuración del recopilador de datos, consulte "Configuración del recopilador de datos de Liberty para aplicaciones IBM Cloud" en la página 916.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Data collectors Reference.

Aplicaciones locales (solo Linux for System x)

- Para obtener información sobre la configuración del recopilador de datos, consulte "Configuración del recopilador de datos para aplicaciones locales" en la página 912.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Data collectors Reference.

Supervisión de WebSphere Infrastructure Manager

Monitoring Agent for WebSphere Infrastructure Manager proporciona las prestaciones de supervisión para el Gestor de despliegue y el Agente de nodo de WebSphere Application Server, incluido el estado del servidor, los recursos y las transacciones. Puede utilizar los datos recopilados por el agente de WebSphere Infrastructure Manager para analizar el rendimiento del Gestor de despliegue y el Agente de nodo y averiguar si se ha producido un problema.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de WebSphere Infrastructure Manager" en la página 963.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de WebSphere Infrastructure Manager Reference (Referencia del agente de WebSphere Infrastructure Manager).

Supervisión de WebSphere MQ

Con Monitoring Agent for WebSphere MQ puede recopilar y analizar fácilmente datos específicos de WebSphere MQ para los gestores de colas desde un único punto privilegiado. Puede hacer un seguimiento de las tendencias de los datos recopilados y resolver los problemas del sistema mediante los paneles de instrumentos predefinidos.

- Si desea más información sobre cómo configurar el agente después de la instalación, consulte "Configuración de la supervisión de WebSphere MQ" en la página 964.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de WebSphere MQ Reference (Referencia del agente de WebSphere MQ).

- Para obtener información sobre la supervisión de colas de mensajes como parte de la Pila de integración de IBM, consulte "Supervisión de la Pila de integración de IBM" en la página 101.

Supervisión de SO Windows

Monitoring Agent for Windows OS proporciona prestaciones de supervisión para la disponibilidad, el rendimiento y el uso de recursos del entorno del sistema operativo Windows. Además, puede configurar la supervisión de archivos de registro para supervisar archivos de registro de aplicación. Puede recopilar y analizar información específica del servidor, como por ejemplo el rendimiento de la CPU y el sistema operativo, información del disco y análisis de rendimiento, análisis de estado de proceso, datos de sesión de internet, información de registros supervisados, estadísticas de servidor de internet, estadísticas de cola de mensajes, datos de estado de trabajo y de impresora, estadísticas de Remote Access Services e información de servicios. El servicio KNTCMA_FCProvider se instala con el agente.

- Para obtener información sobre la configuración de la supervisión de archivos de registro después de la instalación, consulte "Configuración de la supervisión de archivos de registro del agente de sistema operativo" en la página 656.
- Para obtener información sobre los paneles de instrumentos, los umbrales y los atributos, consulte Agente de sistema operativo Windows Reference (Referencia del agente de sistema operativo Windows).

Características

Las características clave varían según la oferta. Algunas características están disponibles en una o ambas ofertas, en un complemento o mediante la integración con otros productos y componentes.

Supervisión de recursos de aplicación

Utilice agentes de supervisión de recursos para supervisar idiomas y middleware.LA cobertura varía en función de la oferta. Consulte "Capacidades" en la página 54.

Supervisión del sistema operativo

Utilice agentes de supervisión de recursos para supervisar sistemas operativos Linux, UNIX y Windows. Consulte "Capacidades" en la página 54.

Supervisión de archivos de registro

Los agentes de SO contienen una característica para supervisar archivos de registro de aplicación. Esta característica incluye la posibilidad de configurar la supervisión de archivo de registro basado en expresiones regulares.

Por compatibilidad, el agente de sistema operativo consume la siguiente información y formatos:

- Información de configuración y el archivo de formato que ha utilizado el agente IBM Tivoli Monitoring Log File Agent V6.x
- Información de configuración y series de formato que ha utilizado Tivoli Event Console Log File Adapter

Estas series de formato permiten al agente filtrar los datos de registro de acuerdo con patrones en el archivo de formato y enviar sólo los datos relevantes a un consumidor de sucesos. El agente de sistema operativo envía datos al Servidor de Cloud APM o a través de Event Integration Facility (EIF) a cualquier receptor EIF, como el analizador de Netcool/OMNIbus Probe for Tivoli EIF.

Paneles de instrumentos

Los **Panel de instrumentos del rendimiento de aplicaciones** proporcionan un estado de alto nivel de las aplicaciones del entorno. Vea las áreas de interés seleccionando del navegador o pulsando en un cuadro de resumen para avanzar al nivel siguiente.

Para conocer las características disponibles en cada nivel del panel de instrumentos, consulte "Todas mis aplicaciones – Panel de instrumentos del rendimiento de aplicaciones" en la página 1113, "Aplicación – Panel de instrumentos del rendimiento de aplicaciones" en la página 1116 y "Grupo e instancia – Panel de instrumentos del rendimiento de aplicaciones" en la página 1121.

Vea los ICR de los dominios de Tivoli Monitoring y Cloud APM en los mismos paneles de instrumentos

En un entorno que incluye los productos IBM Tivoli Monitoring e IBM Cloud Application Performance Management, puede instalar IBM Cloud Application Performance Management Hybrid Gateway para proporcionar una vista consolidada de los sistemas gestionados de ambos dominios. Para ver su entorno híbrido en la Consola de Cloud APM, debe crear un grupo de sistemas gestionados, instalar la Pasarela híbrida en su entorno de Tivoli Monitoring, y configurar las comunicaciones con la Pasarela híbrida.

Para obtener más información, consulte "Integración con IBM Tivoli Monitoring V6.3 " en la página 983.

Medidas históricas

Obtenga visualizaciones de hasta 24 horas de datos históricos en los Panel de instrumentos del rendimiento de aplicaciones. Cuando se visualiza un selector en una pestaña **Visión general** de estado de un panel de instrumentos, puede ajustar el intervalo temporal de los gráficos y las tablas cuyos valores se derivan de muestras de datos históricos. Para los gráficos de líneas, también puede comparar los datos actuales hasta las últimas 24 horas, con hasta 8 días de datos históricos para detectar anomalías.

Para obtener más información, consulte "Ajuste y comparación de métricas a lo largo del tiempo" en la página 1125.

IBM Cloud Application Business Insights Universal View

Puede utilizar Universal View para crear páginas personalizadas para las aplicaciones que está supervisando. Elija entre las diferentes opciones de gráfico y métrica para crear widgets para supervisar datos según sus necesidades. Con Universal View, puede personalizar un panel de instrumentos para ver datos consolidados de varios agentes.

Cuando está viendo datos en el panel de instrumentos, puede cambiar el tipo de gráfico dinámicamente. En el widget de cuadrícula, puede filtrar datos dinámicamente.

Puede exportar los datos de página personalizados a un archivo de datos en bruto.

Para obtener más información, consulte "Vistas personalizadas" en la página 1147.

Detalles de la aplicación

Después de pasar a un panel de instrumentos detallado para una instancia de sistema gestionado en el panel de instrumentos **Todas mis aplicaciones**, se muestra la pestaña Detalles de atributo para crear y gestionar tablas y gráficos de línea históricos personalizados que se pueden guardar. Puede guardar más páginas de tablas o gráficos solo para su visualización o para compartirlos con todos los usuarios en el mismo entorno.

Para obtener más información, consulte el apartado "Creación de una página de tablas o un gráfico personalizados" en la página 1127.

APIs

Las API de Cloud APM están disponibles para la gestión del entorno como, por ejemplo, para asignar roles de usuarios y para crear umbrales. Para obtener más información, consulte "Exploración de las API" en la página 1107.

Control de accesos basado en roles

En Cloud APM, un rol es un grupo de permisos que controla las acciones que puede realizar. Utilice la característica Control de accesos basado en roles para crear roles personalizados, que son la base de la seguridad. Los cuatro roles predefinidos siguientes también están disponibles: Administrador de roles, Administrador de supervisión, Administrador del sistema y Usuario de supervisión. Puede asignar usuarios a roles personalizados o roles predefinidos y los usuarios pueden estar asignados a varios roles. Puede asignar permisos a roles personalizados o puede asignar más permisos a roles predeterminados existentes. Los permisos son acumulativos. A un usuario se le asignan todos los permisos correspondientes a los roles a los que están asignados.

Puede asignar los permisos de visualización y modificación a aplicaciones individuales, grupos de recursos del sistema y grupos de recursos personalizados. Por ejemplo, si es miembro de un rol que

tiene permiso de visualización para una aplicación, puede visualizar todos los componentes de soporte en esa aplicación.

Puede asignar el permiso de visualización y modificación a tareas de administración del sistema. Por ejemplo, si es miembro de un rol que tiene permiso de visualización para Configuración avanzada, puede realizar y guardar cambios en la ventana **Configuración avanzada**.

Para obtener más información, consulte "Roles y permisos" en la página 1036.

Informes históricos
Hay informes disponibles para datos recopilados por el Agente de WebSphere Applications, el Agente de Supervisión de tiempo de respuesta y el Agente de Synthetic Playback. El rastreo de transacciones es necesario para los informes de Agente de Supervisión de tiempo de respuesta (No disponible en Cloud APM, Base) Para descripciones de informes, consulte "Informes" en la página 1158.

Agent Builder
Cree agentes personalizados para supervisar cualquier plataforma o tecnología. Consulte https://www.ibm.com/support/knowledgecenter/SSMKFH/com.ibm.apmaas.doc/install/agent_builder_guide.htm.

Supervisión de recursos de base de datos
LA cobertura varía en función de la oferta. Consulte "Capacidades" en la página 54 para los nombres de las bases de datos que se pueden supervisar.

Supervisión de recursos de infraestructura
Utilice agentes de supervisión de recursos para supervisar hipervisores, almacenamiento y redes.LA cobertura varía en función de la oferta. Consulte "Capacidades" en la página 54.

Supervisión de recursos de aplicaciones comerciales
Utilice agentes de supervisión de recursos para supervisar aplicaciones empresariales y de colaboración.LA cobertura varía en función de la oferta. Consulte "Capacidades" en la página 54.

Supervisión de la experiencia de usuario final y tiempo de respuesta
Consulte qué experimentan los usuarios de la infraestructura en sus dispositivos. Utilice la supervisión del tiempo de respuesta para supervisar el rendimiento y la disponibilidad de sitios web y aplicaciones web del navegador a través de la base de datos y para supervisar dispositivos móviles. Después de instalar el Agente de Supervisión de tiempo de respuesta en los servidores web que desea supervisar, los datos recopilados por estos agentes se visualizan en el Panel de instrumentos del rendimiento de aplicaciones con muy poca, o ninguna, configuración adicional. Los datos del Agente de Supervisión de tiempo de respuesta se utilizan en los paneles de instrumentos de **Transacciones de usuario final**. En Cloud APM, Advanced, puede medir el tiempo de respuesta del navegador, y los datos del Agente de Supervisión de tiempo de respuesta también se utilizan en la **Topología de transacciones agregada**. Para obtener más información, consulte "Escenario: Supervisión de la Pila de aplicaciones Java de IBM " en la página 93.

Rastreo de transacciones
Esta característica no está disponible en Cloud APM, Advanced. La característica de rastreo de transacciones permite la supervisión de transacciones a nivel de instancias y vistas de topología. El rastreo de transacciones se instala como parte de Servidor de Cloud APM. El rastreo de transacciones se habilita automáticamente para algunos agentes, pero se debe habilitar manualmente para otros. Tabla 4 en la página 75 proporciona más información sobre los agentes que dan soporte al rastreo de transacciones.

Tabla 4. Habilitación del rastreo de transacciones para agentes y recopiladores de datos

Despliegue de agentes o recopilador de datos	Habilitado de forma predeterminada	Cómo habilitar
Agente de DataPower	✔	"Configuración del rastreo de transacciones para el Agente de DataPower " en la página 251

Tabla 4. Habilitación del rastreo de transacciones para agentes y recopiladores de datos (continuación)

Despliegue de agentes o recopilador de datos	Habilitado de forma predeterminada	Cómo habilitar
Agente de IBM Integration Bus	—	"Configuración del rastreo de transacciones para el Agente de IBM Integration Bus" en la página 299 **Nota:** TT no está soportado si despliega este agente en Solaris X86.
Recopilador de datos de J2SE	✓	"Configuración de la supervisión de J2SE" en la página 468
Agente de JBoss	—	"Configurar el recopilador de datos de rastreo de transacciones del Agente de JBoss" en la página 486
Recopilador de datos de Liberty	✓	"Configuración del recopilador de datos para aplicaciones locales" en la página 912"Configuración del recopilador de datos de Liberty para aplicaciones IBM Cloud" en la página 916
Agente de Microsoft .NET	—	"Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones" en la página 545
Recopilador de datos de Node.js	—	"Personalización del recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud" en la página 617 "Personalización del Recopilador de datos de Node.js para aplicaciones locales" en la página 623
Agente de Supervisión de tiempo de respuesta + Agente de HTTP Server	—	"Planificación de la instalación " en la página 712
Agente de SAP NetWeaver Java Stack	—	"Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones" en la página 797
Agente de Tomcat	—	"Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones" en la página 835
Agente de WebLogic	—	"Configuración de la supervisión de WebLogic" en la página 846
Agente de WebSphere Applications	—	"Configuración interactiva del recopilador de datos" en la página 870 **Nota:** TT no está soportado si despliega este agente en Solaris X86.

Tabla 4. Habilitación del rastreo de transacciones para agentes y recopiladores de datos (continuación)

Despliegue de agentes o recopilador de datos	Habilitado de forma predeterminada	Cómo habilitar
Agente de WebSphere MQ	–	"Configuración del rastreo de transacciones para el Agente de WebSphere MQ" en la página 973 **Nota:** TT no está soportado si despliega este agente en Solaris X86.

Los datos se muestran en las vistas **Topología de transacciones agregada** y **Topología de instancia de transacción** para todos los agentes que dan soporte al rastreo de transacciones.

Topología de aplicación
Vea cómo están conectados todos los componentes en su entorno de aplicación. Para obtener más información, consulte "Aplicación – Panel de instrumentos del rendimiento de aplicaciones" en la página 1116.

Topología de instancia de transacción
Visualice la ruta que se ha seguido en el entorno para cada instancia de una transacción. Para obtener más información, consulte "Topología de instancia de transacción " en la página 99

Availability Monitoring
IBM Cloud Availability Monitoring proporciona una supervisión sintética mejorada de las aplicaciones web desde varios puntos de presencia alrededor del mundo. Cree pruebas sintéticas que simulan el comportamiento del usuario a intervalos regulares. Ejecute sus pruebas desde puntos de presencia públicos o descargue y despliegue sus propios puntos de presencia en servidores locales o privados. Utilice el panel de instrumentos Availability Monitoring para supervisar la disponibilidad, el rendimiento y las alertas de la aplicación mediante gráficos, tablas de desglose y vistas de mapa. Utilice el análisis en cascada para identificar cuándo se producen problemas de rendimiento y disponibilidad y averiguar las razones de esos problemas.

Para obtener más información acerca de cómo usar pruebas sintéticas, consulte "Availability Monitoring" en la página 1081.

Diagnóstico en profundidad
Para agentes específicos, puede pasar de los paneles de instrumentos de resumen a los paneles de instrumentos de diagnóstico detallado y visualizar información sobre solicitudes individuales. Pase a un mayor nivel de detalle en los paneles de instrumentos de resumen para visualizar detalles a nivel de código, rastreo de pila y consulta SQL. Utilice los paneles de instrumentos de diagnóstico detallado para identificar qué solicitudes tienen un problema y depurar la transacción problemática. También puede detectar, diagnosticar y terminar transacciones colgadas o lentas que siguen en curso (consulte la Referencia de Agente de WebSphere Applications). Tabla 5 en la página 78 proporciona más información sobre los agentes de diagnóstico.

Tabla 5. Paneles de instrumentos de diagnósticos de agentes y recopiladores de datos

Agente o recopilador de datos	**Datos de diagnóstico configurados de forma predeterminada**	**Paneles de instrumentos de diagnóstico detallado disponibles**	**Cómo acceder a los paneles de instrumentos de diagnóstico**	**Cómo configurar el agente o el recopilador de datos para recopilar datos de diagnóstico**
Recopilador de datos de J2SE	✓	Detalle, Módulos web, Instancias de solicitud, Resumen de solicitudes, Rastreos de solicitud	Pulse **Diagnosticar** en el panel de instrumentos **Visión general** o en el panel de instrumentos **Módulos web**.	"Configuración de la supervisión de J2SE" en la página 468
Agente de JBoss	—	Panel de instrumentos de diagnósticoResumen de solicitudes en curso, Panel de instrumentos Rastreo de pila de solicitudes en curso, Recogida de basura de JVM, Comparación de volcado de almacenamiento dinámico	Pulse **Diagnosticar**, **Solicitudes en curso**, **Detalles** o **Vuelco de almacenamiento dinámico** en el panel **Visión general**.	"Configurar el recopilador de datos de rastreo de transacciones del Agente de JBoss" en la página 486
Recopilador de datos de Liberty	✓	Detalles, Vuelco de almacenamiento dinámico, Comparación de vuelcos de almacenamiento dinámico, Análisis de memoria	Pulse **Diagnosticar**, **Ver vuelco de almacenamiento dinámico** o **Ver análisis de memoria** en el panel de instrumentos **Visión general**.	• "Configuración del recopilador de datos de Liberty para aplicaciones IBM Cloud" en la página 916 • "Configuración del recopilador de datos para aplicaciones locales" en la página 912
Agente de Microsoft .NET	—	Instancias de solicitud, Resumen de solicitudes, Rastreos de solicitud	Pulse **Diagnosticar** en el panel de instrumentos **Visión general**.	"Habilitación de la recopilación de datos de diagnóstico mediante el mandato configdc" en la página 546

Tabla 5. Paneles de instrumentos de diagnósticos de agentes y recopiladores de datos (continuación)

Agente o recopilador de datos	**Datos de diagnóstico configurados de forma predeterminada**	**Paneles de instrumentos de diagnóstico detallado disponibles**	**Cómo acceder a los paneles de instrumentos de diagnóstico**	**Cómo configurar el agente o el recopilador de datos para recopilar datos de diagnóstico**
Agente de Node.js	✓	Detalles de recogida de basura, Instancias de solicitud, Resumen de solicitudes, Rastreos de solicitud	Pulse **Diagnosticar** en el panel de instrumentos **Visión general**.	"Configuración del Agente de Node.js" en la página 609
Recopilador de datos de Node.js	✓	Detalles de recogida de basura, Instancias de solicitud, Rastreos de solicitud	Pulse **Diagnosticar** o **Detalles de recogida de basura** en el panel de instrumentos Visión general.	• "Configuración del Recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud (anteriormente Bluemix)" en la página 615 • "Configuración del Recopilador de datos de Node.js autónomo para aplicaciones locales" en la página 621
Recopilador de datos de Python	✓	Detalles de solicitudes más lentas, Detalles de instancias de solicitud, Detalles de rastreos de solicitud, Detalles de hebra Python, Recogida de basura de Python, Detalles de almacenamiento dinámico de Python	Pulse **Diagnosticar**, **Detalle de hebras** o **Detalle de memoria** en el panel de instrumentos **Visión general**.	• "Configuración del recopilador de datos de Python para aplicaciones IBM Cloud" en la página 695 • "Configuración del Recopilador de datos de Python para aplicaciones locales" en la página 701

Tabla 5. Paneles de instrumentos de diagnósticos de agentes y recopiladores de datos (continuación)

Agente o recopilador de datos	**Datos de diagnóstico configurados de forma predeterminada**	**Paneles de instrumentos de diagnóstico detallado disponibles**	**Cómo acceder a los paneles de instrumentos de diagnóstico**	**Cómo configurar el agente o el recopilador de datos para recopilar datos de diagnóstico**
Agente de Ruby	—	Detalle de resumen de solicitud, Instancias de solicitud de muestra, Rastreos de solicitud	Pulse **Diagnosticar** en el panel de instrumentos **Visión general**.	"Configuración de la supervisión de Ruby" en la página 743
Recopilador de datos de Ruby	✓	Instancias de solicitud, Resumen de solicitudes, Rastreos de solicitud	Pulse **Diagnosticar** en el panel de instrumentos **Visión general**.	"Configuración del Recopilador de datos de Ruby para aplicaciones de IBM Cloud" en la página 751
Agente de SAP NetWeaver Java Stack	✓	Instancias de solicitud, Resumen de solicitudes, Rastreos de solicitud	Pulse **Diagnosticar** en el panel de instrumentos **Visión general**.	"Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones" en la página 797
Agente de Tomcat	—	Instancias de solicitud, Resumen de solicitudes, Rastreos de solicitud	Pulse **Diagnosticar** en el panel de instrumentos **Visión general**.	"Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones" en la página 835
Agente de WebLogic	—	Panel de instrumentos de diagnósticoResumen de solicitudes en curso, Panel de instrumentos Rastreo de pila de solicitudes en curso, Detalles de recogida de basura de JVM, Vuelco de almacenamiento dinámico, Comparación de vuelcos de almacenamiento dinámico	Pulse **Diagnosticar**, **Ver solicitudes**, **Detalles** o **Vuelco de almacenamiento dinámico** en el panel **Visión general**.	"Configuración de la supervisión de WebLogic" en la página 846

Tabla 5. Paneles de instrumentos de diagnósticos de agentes y recopiladores de datos (continuación)

Agente o recopilador de datos	Datos de diagnóstico configurados de forma predeterminada	Paneles de instrumentos de diagnóstico detallado disponibles	Cómo acceder a los paneles de instrumentos de diagnóstico	Cómo configurar el agente o el recopilador de datos para recopilar datos de diagnóstico
Agente de WebSphere Applications	—	Diagnóstico, Instancia de solicitud, Secuencia de solicitudes, Resumen de solicitudes en curso, Rastreo de pila de solicitudes en curso, Vuelco de almacenamiento dinámico, Comparación de vuelcos de almacenamiento dinámico, Análisis de memoria	Pulse **Diagnosticar**, **Ver solicitudes**, **Ver vuelco de almacenamiento dinámico** o **Ver análisis de memoria** en el panel de instrumentos **Visión general**. el botón **Ver Análisis de memoria** sólo funciona después de habilitar la supervisión de fugas de memoria.	• "Configuración del recopilador de datos con el programa de utilidad de configuración simple" en la página 867 • "Habilitación de la supervisión de fugas de memoria" en la página 909

El botón **Diagnosticar** solo está habilitado cuando hay configurado un diagnóstico detallado para el agente, y si es miembro del rol Administrador de roles, del rol Administrador de supervisión o de algún otro rol personalizado que tenga permiso de visualización para los paneles de instrumentos de diagnósticos.

Umbrales

Con umbrales, puede detectar comportamientos y condiciones de aplicación específicos en función de las definiciones supervisadas activamente. Hay umbrales predefinidos disponibles para cada agente y puede definir umbrales nuevos para la supervisión. Para obtener más información, consulte "Gestor de umbrales" en la página 1019.

Cuando el reenvío de sucesos está configurado, los sucesos se envían al receptor EIF. Puede utilizar la correlación predeterminada entre umbrales y sucesos reenviados al servidor de sucesos o personalizar la correlación de umbrales. Para obtener más información, consulte "Personalización de un suceso para reenviarlo a un receptor EIF" en la página 1025.

En el **Panel de instrumentos del rendimiento de aplicaciones**, después de seleccionar una aplicación, se visualiza la pestaña **Sucesos**. La pestaña **Sucesos** muestra los sucesos abiertos para la aplicación actual. Puede avanzar a paneles de instrumentos detallados con medidas de rendimiento para ayudarle a determinar la causa del suceso. Para obtener más información, consulte "Estado de suceso" en la página 1143.

Grupos de recursos

Los sistemas gestionados de la empresa supervisada se pueden categorizar en función de su objetivo. Dichos sistemas gestionados tienen a menudo los mismos requisitos de umbral. Utilice el Gestor de grupos de recursos para organizar sistemas supervisados en grupos a los que pueda asignar umbrales

de sucesos. Para obtener más información, consulte “Gestor de grupos de recursos” en la página 1014.

Página Cómo empezar

Después de iniciar la sesión en la Consola de Cloud APM, se accede a la página Cómo empezar. Pulse cualquiera de las **Tareas de usuario** o **Tareas del administrador** para acceder a una visita guiada o una demostración en vídeo basadas en un caso de ejemplo. Los enlaces "Empezar ahora" le llevan directamente a la característica, como por ejemplo el Gestor de umbrales. Los enlaces de **Recursos de la comunidad** llevan a **Preguntas frecuentes**, el foro de Cloud APM y otros.

Están disponibles características adicionales a través de la integración con otros productos y componentes. Si desea más información, consulte “Integración ” en la página 82 y más detalles en Capítulo 8, “Integración con otros productos y componentes”, en la página 983.

Integración

Se proporcionan características adicionales a través de la integración con otros productos y componentes: Tivoli Monitoring, OMEGAMON, Netcool/OMNIbus, Operations Analytics - Log Analysis, Operations Analytics - Predictive Insights, Alert Notification, Control Desk, IBM Cloud y Agent Builder.

IBM Tivoli Monitoring

Se da soporte a la coexistencia de agentes. Puede instalar agentes de IBM Cloud Application Performance Management en el mismo sistema donde están instalados los agentes de IBM Tivoli Monitoring. Sin embargo, ambos tipos de agente no se pueden instalar en el mismo directorio.Si desea más información, consulte “Coexistencia del agente de Cloud APM y el agente de Tivoli Monitoring” en la página 984.

Si su entorno incluye los productos IBM Tivoli Monitoring y Cloud APM (local, en la nube, o ambos), puede instalar IBM Cloud Application Performance Management Hybrid Gateway para proporcionar una vista consolidada de los sistemas gestionados de ambos entornos. Para obtener más información, consulte “Pasarela híbrida” en la página 987. Para obtener la lista actual de agentes de Tivoli Monitoring soportados, consulte Agentes soportados por la pasarela híbrida (APM Developer Center).

IBM OMEGAMON

z Systems Extension Pack conecta uno o varios agentes de OMEGAMON ejecutados en el sistema principal z Systems a Cloud APM. Utilizando z Systems Extension Pack e Pasarela híbrida para conectar los agentes de OMEGAMON desplegados a Cloud APM, puede visualizar datos y sucesos de supervisión para los componentes de la aplicación OMEGAMON en la Consola de Cloud APM.

Para obtener más información, consulte “Integración con OMEGAMON” en la página 999.

IBM Netcool/OMNIbus

Puede reenviar los sucesos desde Cloud APM a su gestor de sucesos de Netcool/OMNIbus in situ. Para obtener más información, consulte “Integración con Netcool/OMNIbus” en la página 999.

IBM Operations Analytics - Log Analysis

Cuando el entorno incluye IBM Operations Analytics - Log Analysis, puede juntar los datos de registro y de rendimiento de aplicaciones para ayudarle a encontrar la causa raíz de los problemas experimentados por las aplicaciones. Puede buscar en los datos de registro asociados a sus aplicaciones para encontrar la causa de un problema, como lentitud o anomalía. Para obtener más información, consulte “Integración con Operations Analytics - Log Analysis” en la página 1004.

IBM Operations Analytics - Predictive Insights

Operations Analytics - Predictive Insights analiza datos y aprende el comportamiento normal de un sistema. Crea un modelo de rendimiento y lo utiliza para detectar o prever un comportamiento fuera del rango modelado y regenera alarmas cuando se produce un comportamiento anómalo. Puede añadir Operations Analytics - Predictive Insights a su suscripción de Cloud APM. A continuación, podrá ver anomalías en el Panel de instrumentos del rendimiento de aplicaciones y descender hasta la interfaz de usuario de Operations Analytics - Predictive Insights para ver más detalles. Para obtener más información, consulte “Integración con Operations Analytics - Predictive Insights” en la página 1005.

IBM Cloud

Puede ver información de supervisión de sus aplicaciones dentro del entorno de IBM Cloud mediante los recopiladores de datos autónomos. Los recopiladores de datos de permiten la integración de prestaciones de supervisión con IBM Cloud mediante la transferencia de datos de supervisión de recursos y diagnóstico detallado profundidad acerca de las aplicaciones IBM Cloud al Servidor de Cloud APM. El Servidor de Cloud APM recibe y procesa la información de supervisión recogida por los recopiladores de datos. Pueden supervisarse los siguientes tipos de aplicaciones IBM Cloud:

- Aplicaciones Liberty
- Aplicaciones Node.js
- Aplicaciones Python
- Aplicaciones Ruby

Después de configurar un recopilador de datos, podrá ver los datos de supervisión en la Consola de Cloud APM. Para obtener más información, consulte "Procedimiento general para configurar recopiladores de datos" en la página 192.

IBM Alert Notification

Si está utilizando IBM Cloud Application Performance Management, IBM Alert Notification se integra automáticamente. Alert Notification es un sistema de notificación simple y fácil de usar que proporciona al personal de TI notificación instantánea de las alertas de problemas del entorno de operaciones de TI. Los datos recibidos de los agentes proporcionan el origen de las alertas. Después de activar Alert Notification, conéctelo a una instancia de Cloud APM. Como paquete autónomo, puede integrar Alert Notification con cualquier herramienta de supervisión en las instalaciones que pueden implementar e instalar una API REST. Las herramientas soportadas incluyen IBM Tivoli Netcool/OMNIbus. Para obtener más información, consulte Integración con Alert Notification.

IBM Control Desk

La integración con IBM Control Desk está disponible enviando un tíquet de soporte a IBM Support. Puede configurar los sucesos de Cloud APM para abrir automáticamente tíquets en IBM Control Desk. Vaya a IBM Support y seleccione **Suscripción**. Para obtener más información sobre los detalles que debe proporcionar al soporte técnico para permitirles configurar esta integración, consulte "Integración con Control Desk" en la página 1007.

IBM Agent Builder

Puede utilizar Agent Builder para crear agentes personalizados para cualquier tecnología. Para obtener más información, consulte https://www.ibm.com/support/knowledgecenter/SSMKFH/com.ibm.apmaas.doc/install/agent_builder_guide.htm.

Documentación

Puede buscar información para IBM Cloud Application Performance Management en IBM Knowledge Center, la Consola de Cloud APM y Application Performance Management Developer Center.

IBM Knowledge Center

Cloud APM en IBM Knowledge Center es la fuente oficial de información técnica del producto.

Ayuda de la interfaz de usuario

Cuando ha iniciado la sesión en la Consola de Cloud APM o explora Demostración guiada, puede acceder al sistema de ayuda:

- Pulse **Contenido de la ayuda** en la barra de navegación. Menú de ayuda.
- Pulse en el banner de Panel de instrumentos del rendimiento de aplicaciones.
- Pulse el enlace **Más información** en las páginas Configuración del sistema.
- Pulse en el widget del panel de instrumentos.

IBM Application Performance Management Developer Center
Application Performance Management Developer Center es una ubicación central para una gran variedad de contenido de APM aplicable a una amplia gama de usuarios de APM. El contenido incluye documentación, blogs, vídeos y enlaces a recursos adicionales.

Foro y dwAnswers de IBM Cloud Application Performance Management
Los Foro de Cloud Application Performance Management y dwAnswers contienen debates técnicos de problemas del producto, que incluyen la resolución de problemas y soluciones.

También hay información disponible en los sitios web siguientes:

Herramienta Informes de compatibilidad de productos de software (SPCR)
Puede utilizar la herramienta SPCR para generar varios tipos de informes relacionados con las ofertas oferta y los requisitos de componentes. Busque uno de los nombres de oferta de Cloud Application Performance Management o de IBM Cloud Application Performance Management - Agents.

IBM Marketplace
Recursos tales como demostraciones en vídeo y preguntas más frecuentes (FAQ) están disponibles en IBM Marketplace.

IBM API Explorer
Para obtener información sobre las APIs de Cloud APM, consulte “Exploración de las API” en la página 1107.

Terminología de IBM
El sitio web Terminología de IBM contiene la terminología relevante de los productos IBM consolidada en una ubicación para mayor comodidad.

IBM Redbooks
El sitio web de IBM Redbooks contiene publicaciones Redbooks, Redpapers y notas técnicas de Redbooks que proporcionan información acerca de los productos desde las perspectivas de la plataforma y la solución.

Convenciones utilizadas en la documentación

Se utilizan varias convenciones en la documentación para términos, acciones, mandatos y vías de acceso especiales que dependen del sistema operativo y para información específica de la plataforma y del producto.

Convenciones de tipo de letra

En la documentación se utilizan las siguientes convenciones de tipo de letra:

Negrita

- Comandos en minúsculas, mandatos en mayúsculas y minúsculas, parámetros y variables de entorno que son difíciles de distinguir del texto circundante
- Controles de interfaz (recuadros de selección, botones, botones de selección, selectores cíclicos, campos, carpetas, iconos, recuadros de lista, elementos dentro de recuadros de lista, listas de varias columnas, contenedores, opciones de menú, nombres de menú, pestañas, hojas de propiedades), etiquetas (como **Sugerencia:**)
- Palabras clave y parámetros del texto

Cursiva

- Citas (ejemplos: títulos de publicaciones, disquetes y discos CD)
- Palabras y frases definidas en el texto (ejemplo: una línea no conmutada se denomina una *línea punto a punto*)
- Resaltado de palabras y letras (ejemplo: la dirección de LUN debe comenzar por la letra *L*).
- Nuevos términos en el texto, excepto en una lista de definiciones (por ejemplo: una *vista* es un marco en un espacio de trabajo que contiene datos).
- Variables y valores que se deben proporcionar (ejemplo: donde *minombre* representa...)

`Monoespaciado`

- Ejemplos y códigos de ejemplo
- Nombres de archivo, nombres de directorio, nombres de ruta, directivas de programación, propiedades y otros elementos que son difíciles de distinguir del texto circundante
- Texto de mensajes y solicitudes
- Texto que debe escribir el usuario
- Valores para argumentos u opciones de mandatos

`Negrita monoespaciado`

- Nombres de mandatos y nombres de macros y programas de utilidad que se pueden escribir como mandatos
- Nombres de variables de entorno en el texto
- Palabras clave
- Nombres de parámetros en el texto: parámetros de estructura de API, parámetros y argumentos de mandato y parámetros de configuración
- Nombres de procesos
- Nombres de variables de registro en el texto
- Nombres de scripts

Variables y vías de acceso dependientes del sistema operativo

La dirección de la barra inclinada de las rutas de directorio puede variar en la documentación. Independientemente de lo que pueda verse en la documentación, siga estas directrices:

- Linux AIX Utilice una barra diagonal (**/**).
- Windows Utilice una barra inclinada invertida (****).

Los nombres de las variables de entorno no siempre son los mismos en Windows y AIX. Por ejemplo, %TEMP% en Windows es equivalente a $TMPDIR en AIX or Linux.

Para variables de entorno, siga estas directrices:

- Linux AIX Utilice **$***variable*.
- Windows Utilice **%***variable***%**.

Windows Si está utilizando el shell Bash en un sistema Windows, puede utilizar las convenciones AIX.

Directorio de instalación variable y vías de acceso para los agentes

dir_instalación es el directorio de instalación para los agentes. La ubicación predeterminada depende del sistema operativo:

- Windows `C:\IBM\APM`
- Linux `/opt/ibm/apm/agent`
- AIX `/opt/ibm/apm/agent`

Capítulo 4. Planificación del despliegue

Para asegurarse de que el despliegue de IBM Cloud Application Performance Management es satisfactorio, la planificación es crítica.

Requisitos del sistema

Para los agentes y recopiladores de datos de IBM Cloud Application Performance Management, se da soporte a varios sistemas operativos y cada uno de esos componentes tiene requisitos específicos.

Huso horario

Utilice NTP (Network Time Protocol) en sistemas gestionados para asegurar que la hora sea precisa. Establecer la hora para que coincida con la ubicación física de los servidores (por ejemplo, UTC-03:00 para Brasilia y UTC +06:30 para Yangon) ayuda a asegurar indicaciones de fecha y hora exactas para sucesos y transacciones. Los agentes informan de datos en la UI de APM en la hora local del usuario.

Requisitos de agente y recopilador de datos de Cloud APM
Obtenga información sobre los requisitos para cada agente de supervisión y recopilador de datos autónomo que tenga previsto instalar.

El agente y el recopilador de datos de Cloud APM son en general son transparentes con el hipervisor, lo que significa que se pueden instalar y desplegar en cualquier sistema operativo independientemente de los hipervisores en los que estén alojados los sistemas operativo como, por ejemplo, Hyper-V, IBM PowerVM, KVM, VMWare ESX, etc.

Para conocer los requisitos de los agentes y los recopiladores de datos, utilice los enlaces de la sección Component reports de System requirements (APM Developer Center).

Para obtener información actualizada sobre los navegadores soportados, consulte el informe IBM Cloud Application Performance Management Detailed System Requirements.

También puede buscar IBM Cloud Application Performance Management en la herramienta Informes de compatibilidad de productos de software.

El sistema local donde está instalado el agente debe admitir la codificación UTF-8 si el agente envía datos globalizados al Servidor de Cloud APM.

Puertos predeterminados utilizados por los agentes y recopiladores de datos

Diversos puertos se utilizan para la comunicación entre el componente Cloud APM y la aplicación o sistema (local o remoto) que se está supervisando. En la mayoría de los casos, se suministran puertos predeterminados para facilitar la configuración. La mayoría de los valores predeterminados pueden personalizarse mediante parámetros de configuración.

La Tabla 6 en la página 88 lista los puertos predeterminados utilizados por los agentes y recopiladores de datos de Cloud APM para comunicarse con las aplicaciones o sistemas que estén supervisando. En la tabla, N/A indica una de las situaciones siguientes:

- El agente o recopilador de datos no utiliza ningún puerto para comunicarse con la aplicación o el sistema supervisado.
- El puerto utilizado para la comunicación está determinado por la configuración de la aplicación supervisada.
- Los puertos utilizados por el agente o recopilador de datos se asignan dinámicamente y no se suministran valores predeterminados estáticos.
- Todos los puertos que deben utilizarse deben ser especificados por el usuario y no se suministran valores predeterminados.

Tabla 6. Puertos predeterminados utilizados por los agentes y recopiladores de datos

Agentes y recopiladores de datos	Puertos predeterminados	Configurable	Local	Remoto
Agente de Amazon EC2	• Puerto TCP 80 (para HTTP) • Puerto TCP 443 (para HTTPS)	N/A	Sí	No
Agente de Amazon ELB	• Puerto TCP 80 (para HTTP) • Puerto TCP 443 (para HTTPS)	N/A	No	No
Agente de Azure Compute	• Puerto TCP 80 (para HTTP) • Puerto TCP 443 (para HTTPS)	No	No	No
Agente de Cassandra	7199 (para servidor JMX, local y remoto)	Sí	Sí	Sí
Agente de Cisco UCS	• Puerto TCP 80 (para HTTP) • Puerto TCP 443 (para HTTPS)	No	Sí	No
Agente de Citrix VDI	Para llamadas PowerShell: • 5985 (para HTTP) • 5986 (para HTTPS)	Sí	Sí	Sí
Agente de Db2	• 50000 (puerto predeterminado de servidor de Db2) • Supervisión remota soportada: utiliza el número de puerto indicado por el usuario al catalogar la instancia de servidor remoto.	Sí	Sí	Sí
Agente de DataPower	5550 (para conectarse a un dispositivo DataPower remoto)	Sí	No	Sí
Agente de Hadoop	• Supervisión local: valor de la variable de entorno **CP_PORT** • Supervisión remota: – 50070 (Namenode en espera) – 50090 (Namenode secundario) – 8088 (ResourceManager) – 19888 (JobHistory Server) – 8080 (Ambari)	Sí	Sí	Sí
Agente de HMC Base	12443 (para descargar el SDK de HMC)	No	Sí	No
Agente de HTTP Server	El servidor HTTP se puede configurar en un puerto distinto, pero el agente en sí no tiene ningún puerto predeterminado.	N/A	Sí	No
Agente de IBM Cloud	Conexión de salida a api.softlayer.com puerto 443.	N/A	No	Sí

Tabla 6. Puertos predeterminados utilizados por los agentes y recopiladores de datos (continuación)

Agentes y recopiladores de datos	Puertos predeterminados	Configurable	Local	Remoto
Agente de IBM Integration Bus	N/A	N/A	Sí	No
Internet Service Monitoring	Para databridge: • 9510 • 9520	Sí	No	Sí
Agente de DataStage	• 9443 (puerto HTTPS de WAS) • 50000 (puerto JDBC de base de datos) • 1433 (Microsoft SQL) • 1521 (Oracle)	Sí	Sí	Sí
Recopilador de datos de J2SE	N/A	N/A	No	No
Agente de JBoss	Varía según la versión del servidor JBoss: • 9990 • 9994 • 9999	No	Sí	No
Recopilador de datos de Liberty	N/A	N/A	No	No
Agente de Linux KVM	• 8080 (para HTTP) • 8443 (para HTTPS)	Sí	Sí	No
Agente de sistema operativo Linux	22 (para la supervisión de registro remoto con SSH)	Sí	Sí	No
Agente de MariaDB	3306	Sí	Sí	Sí
Agente de Microsoft Active Directory	El número de puerto depende del valor de escucha para el uso de supervisión.	N/A	Sí	Sí
Agente de Microsoft Cluster Server	N/A	N/A	No	No
Agente de Microsoft Exchange Server	N/A	N/A	No	No
Agente de Microsoft Hyper-V Server	N/A	N/A	No	No
Agente de Microsoft IIS	N/D	N/D	No	No
Agente de Microsoft .NET	Para enviar datos de rastreo de transacciones, se utiliza el puerto 5456 de forma predeterminada.	Sí	Sí	No
Agente de Microsoft Office 365	7799 (para la transacción sintética Skype)	Sí	Sí	No

Tabla 6. Puertos predeterminados utilizados por los agentes y recopiladores de datos (continuación)

Agentes y recopiladores de datos	Puertos predeterminados	Configurable	Local	Remoto
Agente de Microsoft SharePoint Server	1433 (para servidor SQL)	No	Sí	Sí
Agente de Microsoft SQL Server	1433 (predeterminado del servidor SQL)	Sí (por **COLL_PORT**)	Sí	No
Agente de MQ Appliance	• 162 (para recibir sucesos de SNMP) • 5554 (para conectar a MQ Appliances)	Sí	Sí	Sí
Agente de MongoDB	• 27017 (para instancia única) • 27019 (para clúster)	Sí	Sí	No
Agente de MySQL	3306 (para conexión JDBC)	Sí	Sí	Sí
Agente de NetApp Storage	Para la supervisión remota: • 8088 • 8488 • 443 • 8443	No	No	Sí
Agente de Node.js	63336	Sí	Sí	No
Recopilador de datos de Node.js	N/D	N/D	No	No
Agente de OpenStack	5000 (para conectar el servicio de identidad de OpenStack)	Sí	No	Sí
Agente de Oracle Database	1521 (para conexión SQL)	Sí	Sí	No
Agente de PHP	• Conexión de Apache • El número de puerto se basa en la configuración de Apache	Sí	Sí	No
Agente de PostgreSQL	5432 (para conexión JDBC)	Sí	Sí	Sí
Recopilador de datos de Python	N/D	N/D	No	No
Agente de RabbitMQ	Número de puerto en el que el plug-in de gestión de RabbitMQ está habilitado (local y remoto): 15672	Sí	Sí	Sí
Agente de Supervisión de tiempo de respuesta	• El modelo de analizador de paquetes supervisa transacciones HTTP en el puerto 80. • El modelo de servidor HTTP supervisa todos los puertos.	Sí	Sí	No
Agente de Ruby	Se genera dinámicamente	N/A	Sí	No

Tabla 6. Puertos predeterminados utilizados por los agentes y recopiladores de datos (continuación)

Agentes y recopiladores de datos	Puertos predeterminados	Configurable	Local	Remoto
Recopilador de datos de Ruby	N/D	N/D	No	No
Agente de SAP	33*nn* (donde *nn* es el número de instancia de SAP)	No	Sí	No
Agente de SAP HANA Database	Valor predeterminado: 30013. Rango: 30013-39913.	Sí	Sí	No
Agente de SAP NetWeaver Java Stack	Valor predeterminado: 50004. Rango: 50004-59904.	Sí	Sí	No
Agente de Siebel	N/D	N/D	Sí	No
Agente de Skype for Business Server (anteriormente conocido como agente de Microsoft Lync Server)	• Puerto predeterminado de Business server 5061 • Puerto de servidor SQL 1433 (local o remoto en función del entorno).	No	Sí	No
Agente de Sterling Connect Direct	1363	Sí	No	Sí
Agente de Sterling File Gateway	50000 El número de puerto de la API REST de IBM B2B Integrator y el número de puerto de base de datos son necesarios y se pueden configurar.	Sí	Sí	Sí
Agente de Sybase	5000	N/D	Sí	No
Agente de Synthetic Playback	• 4444 (para la conexión de servidor selenium interno) • Los puertos remotos se especifican en el URL http de los sitios web supervisados, generalmente HTTP 80 y HTTPS 443	No	Sí	No
Agente de Tomcat	8686 (para el servidor MBean de Tomcat)	Sí (por puerto JMX)	Sí	No
Agente de sistema operativo UNIX	22 (para la supervisión de registro remoto con SSH)	Sí	Sí	No
Agente de VMware VI	• 443 (para la supervisión remota) • 80 (para la supervisión local)	No	Sí	Sí
Agente de WebLogic	7003 (Tráfico HTTP de gestión de JMX)	Sí	Sí	No

Tabla 6. Puertos predeterminados utilizados por los agentes y recopiladores de datos (continuación)				
Agentes y recopiladores de datos	**Puertos predeterminados**	**Configurable**	**Local**	**Remoto**
Agente de WebSphere Applications	• 63335 (para agente de supervisión V8) • 63336 (para agente de supervisión V6) • 63355 (para supervisión de recursos) • 5457 (para Transaction Framework Extension)	Sí	Sí	No
Agente de WebSphere Infrastructure Manager	N/D	N/A	Sí	No
Agente de WebSphere MQ	El número de puerto depende del valor de escucha para el uso de supervisión.	N/D	No	Sí
Agente de sistema operativo Windows	22 (para la supervisión de registro remoto con SSH)	Sí	Sí	No

Escenarios

En función de la complejidad del entorno, debe instalar distintos agentes para supervisar distintos componentes. Utilice estos escenarios de despliegue como ayuda para comprender qué debe instalar y dónde para obtener los mejores resultados con IBM Cloud Application Performance Management.

Escenario: Supervisión de IBM API Connect

Puede supervisar y resolver los problemas del entorno IBM API Connect mediante los agentes de APM y los recopiladores de datos.

El producto Cloud APM le ayuda a gestionar el rendimiento y la disponibilidad del entorno API Connect. Los recopiladores de datos y los agentes de Cloud APM proporcionan visibilidad y control de la infraestructura de API Connect y las APIs de la aplicación y permiten obtener un rendimiento óptimo y uso eficiente de los recursos. Cuando surgen problemas de rendimiento con el entorno de API Connect, el producto Cloud APM puede ayudarle a detectarlos, diagnosticarlos y aislarlos.

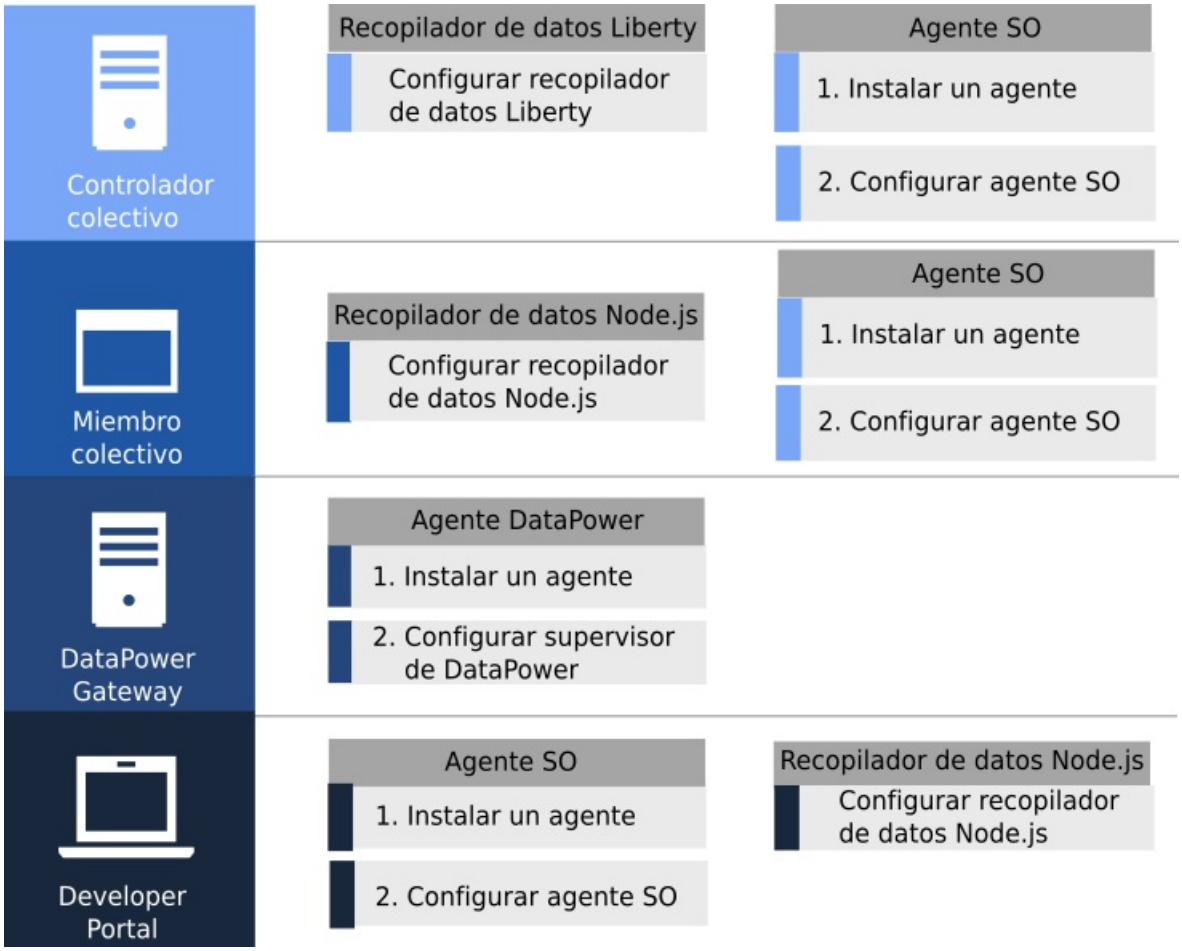
Por ejemplo, puede instalar los agentes de sistema operativo en todos los sistemas aplicables. Utilice los agentes de sistema operativo para recopilar y analizar el rendimiento específico del servidor, incluido el rendimiento de la CPU, la E/S y la utilización de disco, la disponibilidad y el rendimiento de procesos y el rendimiento de red. Además, los agentes de sistema operativo se pueden configurar para supervisar los registros clave de API Connect y del sistema.

Si tiene otros productos de middleware desplegados, la característica de rastreo de transacciones que está instalada como parte del Servidor de Cloud APM, puede proporcionarle vistas de topología para ver la información de rastreo de transacciones para los productos de middleware y los servicios que exponen y resolver problemas cuando surgen.

La imagen siguiente muestra los componentes de API Connect y los recopiladores de datos y los agentes de Cloud APM que pueden supervisarlos. Para habilitar estos agentes y recopiladores de datos, complete las tareas de instalación y configuración que aparecen en la lista bajo el nombre del recopiladores de datos y el agente. Pulse los recuadros rectangulares de la imagen que contienen el nombre de tarea para ir a las tareas de instalación o configuración.

Nota:

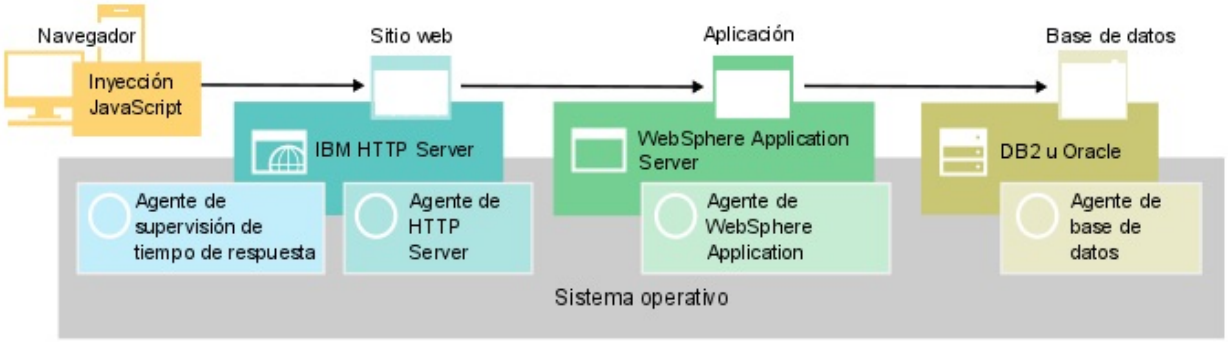
- Instale un Recopilador de datos de Node.js en cada aplicación IBM API Connect del miembro colectivo.
- Al supervisar DataPower Gateway, el Agente de DataPower se ejecuta remotamente desde el dispositivo DataPower.



1. “Configuración del recopilador de datos para aplicaciones locales” en la página 912
2. Capítulo 6, “Instalación de los agentes”, en la página 125
3. “Configuración de la supervisión del sistema operativo” en la página 654
4. “Configuración del Recopilador de datos de Node.js autónomo para aplicaciones locales” en la página 621
5. Capítulo 6, “Instalación de los agentes”, en la página 125
6. “Configuración de la supervisión del sistema operativo” en la página 654
7. Capítulo 6, “Instalación de los agentes”, en la página 125
8. “Configuración de la supervisión DataPower” en la página 240
9. Capítulo 6, “Instalación de los agentes”, en la página 125
10. “Configuración de la supervisión del sistema operativo” en la página 654
11. “Configuración del Recopilador de datos de Node.js autónomo para aplicaciones locales” en la página 621

Escenario: Supervisión de la Pila de aplicaciones Java de IBM

Puede supervisar y resolver problemas de la Pila de aplicaciones Java de IBM para ver la información de supervisión de transacciones desde el navegador a la base de datos, incluida la supervisión de recursos desde componentes individuales. La Pila de aplicaciones Java de IBM incluye IBM HTTP Server, WebSphere Application Server y la base de datos de IBM Db2 u Oracle.



Supervisión de la Pila de aplicaciones Java de IBM
Para supervisar la Pila de aplicaciones Java de IBM, instale los agentes que se listan para cada componente en el orden especificado.

Opcionalmente, si también desea supervisar el sistema, instale agentes de sistema operativo en todos los componentes.

Para el servidor web, realice los pasos siguientes:

1. Instale la Agente de HTTP Server.

   Vía de acceso rápida: Esta instalación instala también Módulo de Tiempo de respuesta de IBM HTTP Server y configura automáticamente la inyección de JavaScript.
2. Configure la instalación del Agente de HTTP Server.
3. Instale el agente de Supervisión de tiempo de respuesta.

Para el servidor de aplicaciones, instale el Agente de WebSphere Applications.

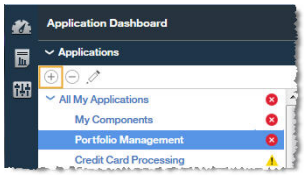
Para la base de datos, instale el agente de base de datos Oracle o el agente de Db2, según su base de datos.

Adición de aplicaciones web al Application Performance Dashboard
Añada las aplicaciones web que desee supervisar al Application Performance Dashboard.

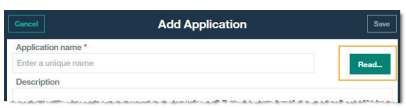
Procedimiento

Para añadir aplicaciones web, realice los pasos siguientes:

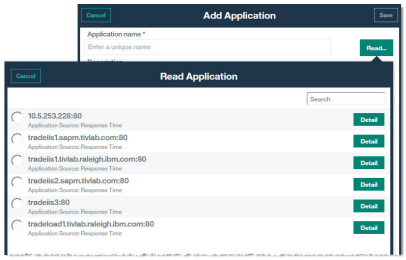
1. En el Application Performance Dashboard, pulse **Añadir aplicación**.



2. Pulse **Lectura** para abrir una lista de aplicaciones descubiertas.



3. Seleccione la aplicación web que desee supervisar.



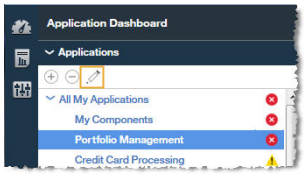
4. Pulse **Guardar**.

Asociación de la Pila de aplicaciones Java de IBM con la aplicación web
Edite la aplicación web para asociar los componentes de base de datos y WebSphere Application Server que desee supervisar con ella.

Procedimiento

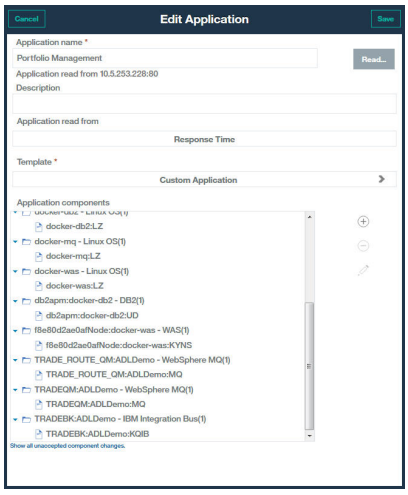
Para visualizar los componentes en Pila de aplicaciones Java, realice los pasos siguientes en el Application Performance Dashboard:

1. Seleccione el servidor web y pulse **Editar aplicación**.



2. En la ventana **Editar aplicación**, pulse **Añadir componentes** +.
3. En la ventana **Seleccionar componente**, seleccione WebSphere Application Server.
4. En **Editor de componentes**, seleccione las instancias del componente necesario y pulse **Añadir**.

   Las instancias de WebSphere Application Server detectadas se añaden automáticamente a esa lista.
5. Pulse **Atrás** y repita los pasos “3” en la página 95 - “4” en la página 95 para la base de datos. Continúe añadiendo instancias de base de datos y WebSphere Application Server hasta que Pila de aplicaciones Java se haya completado.



6. Pulse **Cerrar** y a continuación **Guardar** para volver al Application Performance Dashboard.

Resultados

Consejo: Si la Topología de transacciones agregada no muestra inicialmente la topología que se espera, espere a que esta se renueve y vuélvalo a comprobar en unos minutos. Si la topología sigue sin ser lo que se espera, es posible que su aplicación no se comunique con los componentes esperados. Compruebe su entorno.

Visualización de los resultados de la supervisión de la Pila de aplicaciones Java de IBM
Puede ver los resultados de la supervisión de la Pila de aplicaciones Java de IBM en las topologías.

Acerca de esta tarea

En las topologías verá la información de la supervisión de transacciones del navegador a la base de datos, incluida la supervisión de recursos desde componentes individuales. En la Topología de transacciones agregada y la Topología de instancia de transacción se visualizan los nodos siguientes:

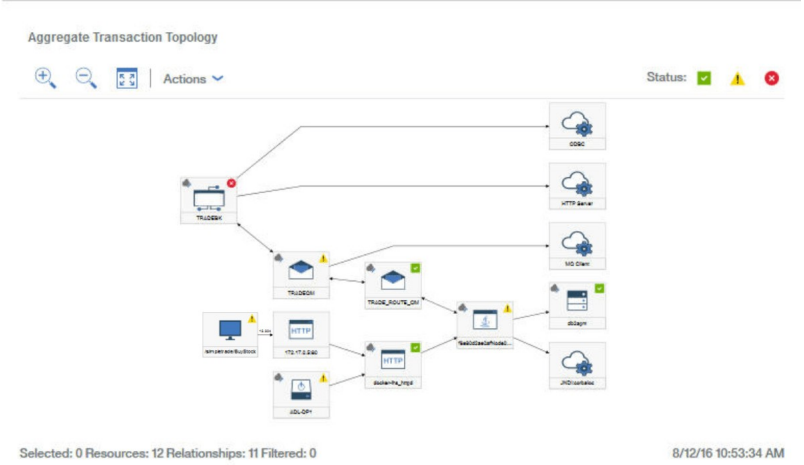
- Navegador, que se visualiza solo cuando la inyección de JavaScript está habilitada
- Servidor HTTP
- WebSphere Application Server
- Base de datos

Procedimiento

Puede enlazar de nodos de la topología a información más detallada sobre ese nodo:

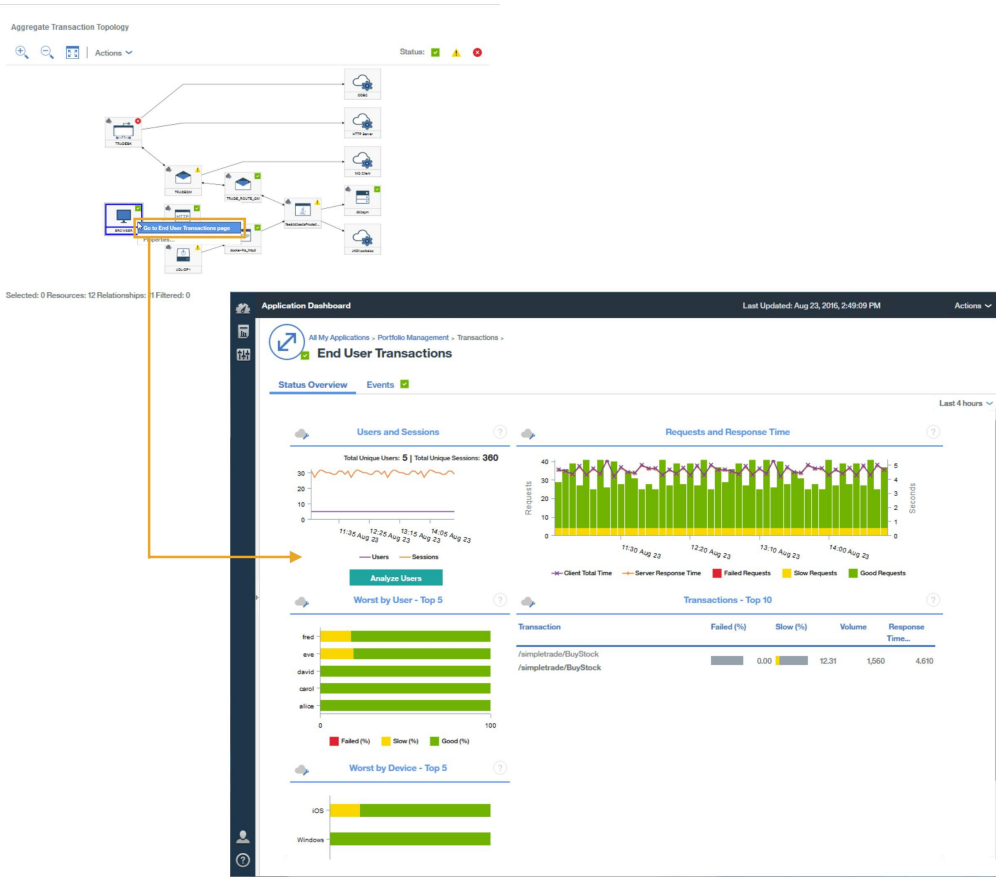
1. Pase el puntero sobre un nodo para visualizar una ventana con información adicional.
2. Para conseguir un panel de instrumentos mucho más detallado, pulse el botón derecho del ratón en el nodo y seleccione el enlace.

Topología de transacciones agregada
La Topología de transacciones agregada se visualiza en el panel de instrumentos Resumen de aplicaciones.



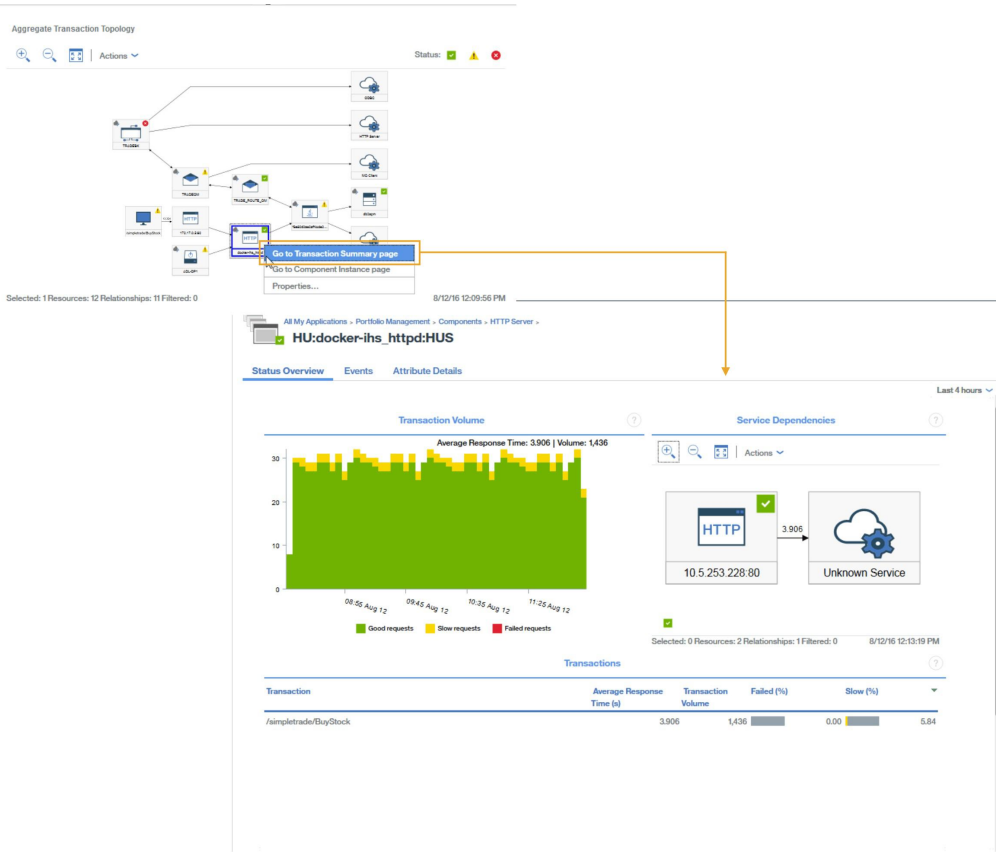
Las topologías de transacciones agregadas visualizan la siguiente información:

- Nodo para clientes basados en navegador, detalle más hasta la experiencia de usuario final



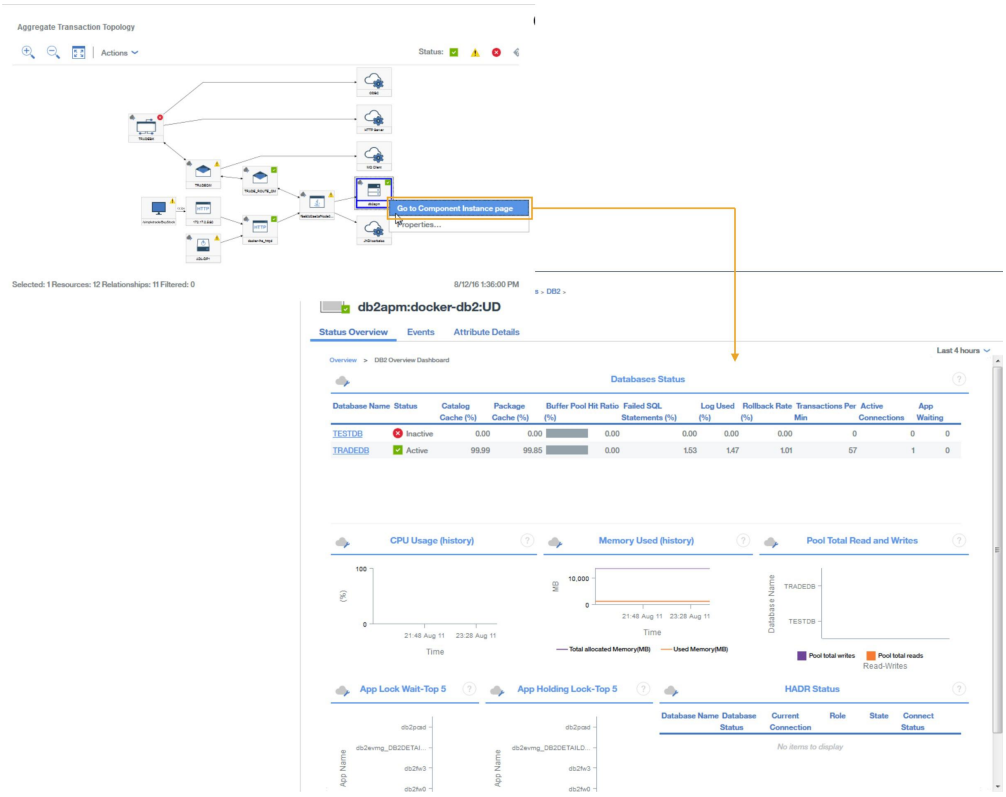
Recuerde: Este nodo solo se visualiza cuando la inyección automática de JavaScript mide los datos del navegador.

- Nodos para aplicaciones basadas en HTTP, detalle más hasta la página de recursos del servidor web



- Nodos para aplicaciones basadas en WebSphere Application Server, descienda a un mayor nivel de detalle hasta una página de recursos de aplicación, o una página de resumen de transacciones

- Nodos para los servidores de base de datos específicos, descienda a un mayor nivel de detalle hasta una página de recursos de base de datos si está disponible

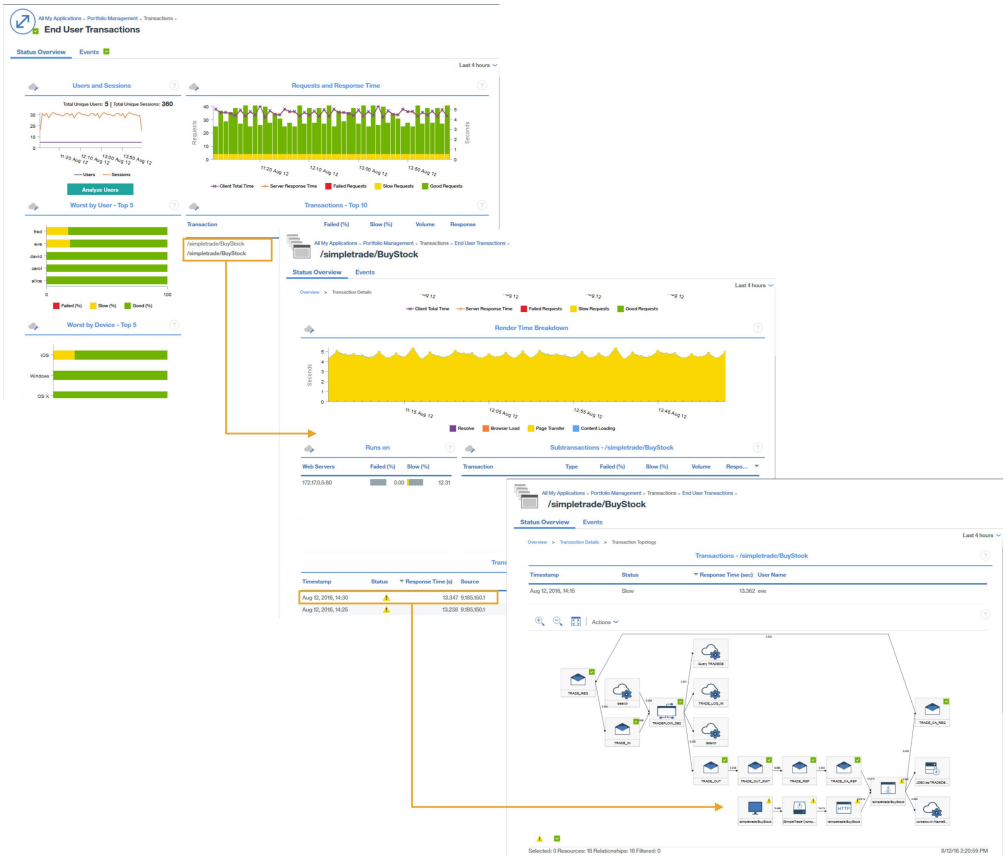


Topología de instancia de transacción

Las topologías de instancia de transacciones se visualizan para transacciones de usuario final reales.

Detalle más en el resumen **Transacciones de usuario final** mediante los widgets siguientes:

1. Seleccione una transacción en la tabla Transacciones - 10 principales
2. Seleccione una instancia en la tabla Instancias de transacciones



Las topologías de instancias de transacciones para la pila de aplicaciones Java muestra los siguientes nodos. Pulse el nodo para visualizar información sobre el mismo.

- Nodo para clientes basados en navegador

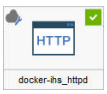
  Recuerde: Este nodo solo se visualiza cuando la inyección automática de JavaScript mide los datos del navegador.
- Nodos HTTP, incluidos tiempos de respuesta del navegador
- Nodos DataPower, si están instrumentados
- Nodos WebSphere Application Server, en los que puede detallar hasta la página de recursos de aplicación
- Nodos de servidor de base de datos, en los que puede detallar hasta un estado de los recursos de base de datos e información de diagnóstico de sentencias SQL para solicitudes JDBC

  Consejo: Cuando la topología indica que la mayor parte del tiempo de respuesta se utiliza en la base de datos, al pulsar **Diagnóstico** se abre directamente la información de sentencias SQL.

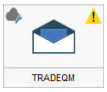
También se visualizan gráficas de Gantt, que resumen la temporización de instancias.

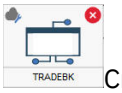
Diagnóstico de problemas en su entorno
Si las instancias de transacciones para uno de los componentes de su entorno son lentas o fallan, se asigna al componente afectado un estado adecuado.

Un nodo puede tener uno de los estados siguientes:

- 

Correcto, el nodo tiene una marca rodeada de un cuadrado verde en la esquina superior derecha

- 

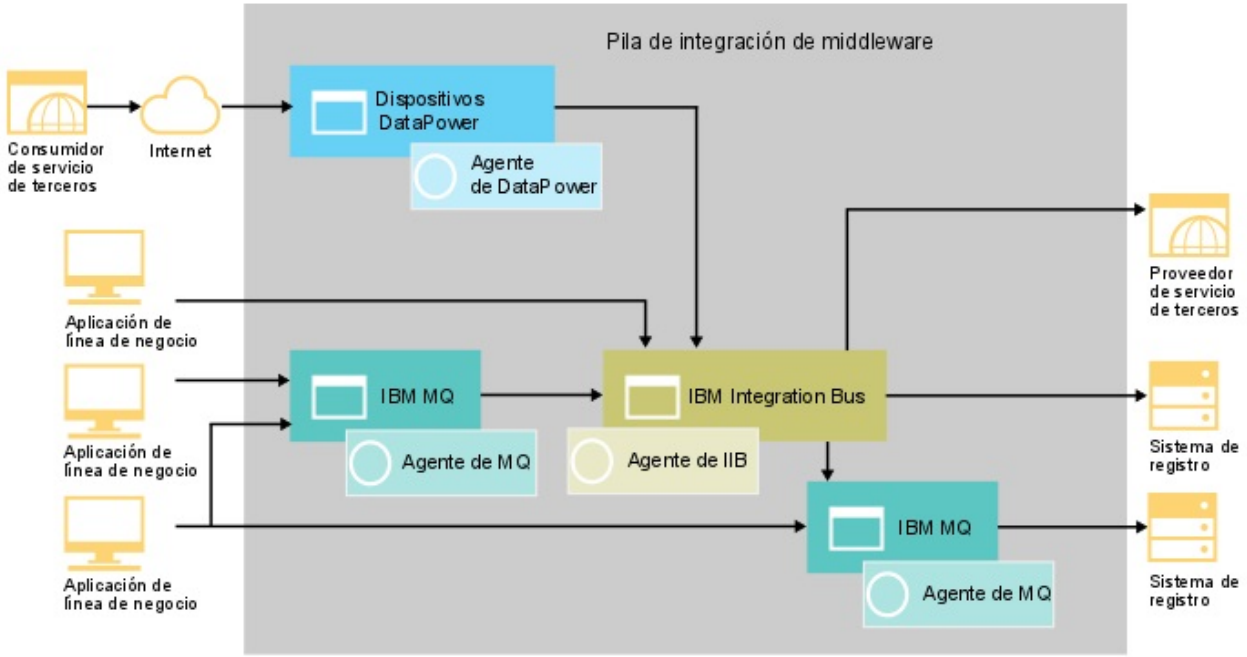
Aviso, el nodo tiene un signo de exclamación rodeado de un triángulo amarillo en la esquina superior derecha
- 

Crítico, el nodo tiene un fondo rojo y una cruz dentro de un círculo rojo en la esquina superior derecha

Para identificar la causa de los problemas de estos componentes con estado de aviso o crítico, pulse con el botón derecho del ratón sobre el nodo y busque la información detallada sobre cuál puede ser la causa de las anomalías.

Escenario: Supervisión de la Pila de integración de IBM

Puede supervisar la Pila de integración de IBM para ver la información de rastreo de transacciones para los productos middleware y los servicios que exponen y resolver problemas si surge alguno. La Pila de integración de IBM incluye IBM MQ, IBM Integration Bus y Dispositivo DataPower.



Supervisión de la Pila de integración de IBM

Para supervisar la Pila de integración de IBM, instale los agentes que se listan para cada componente en el orden especificado.

Opcionalmente, si también desea supervisar un sistema, instale agentes de sistema operativo en ese sistema.

Para IBM MQ, complete los pasos siguientes:

1. Instale el Monitoring Agent for WebSphere MQ.
2. Configure el Agente de WebSphere MQ para conectarse al gestor de colas.
3. Habilite el **rastreo de actividad de aplicación de MQ** en el gestor de colas.

Para IBM Integration Bus, complete los pasos siguientes:

1. Instale el Monitoring Agent for IBM Integration Bus.
2. Habilite IBM Integration Bus para el rastreo de transacciones.
3. Configure el rastreo de transacciones para las instancias de Agente de IBM Integration Bus necesarias.

Para Dispositivo DataPower, complete los pasos siguientes:

1. Instale el Monitoring Agent for DataPower.
2. Configure Agente de DataPower para conectarse a Dispositivo DataPower.
3. Asegúrese de que el rastreo de transacciones esté habilitado para las instancias necesarias de Agente de DataPower .
4. Configure Dispositivo DataPower.

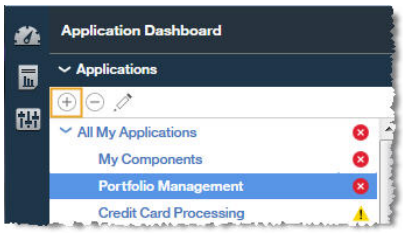
Adición de aplicaciones middleware al Application Performance Dashboard

Cree una aplicación de Pila de integración de IBM y añádale las instancias de IBM MQ, IBM Integration Bus y Dispositivo DataPower que desea supervisar.

Procedimiento

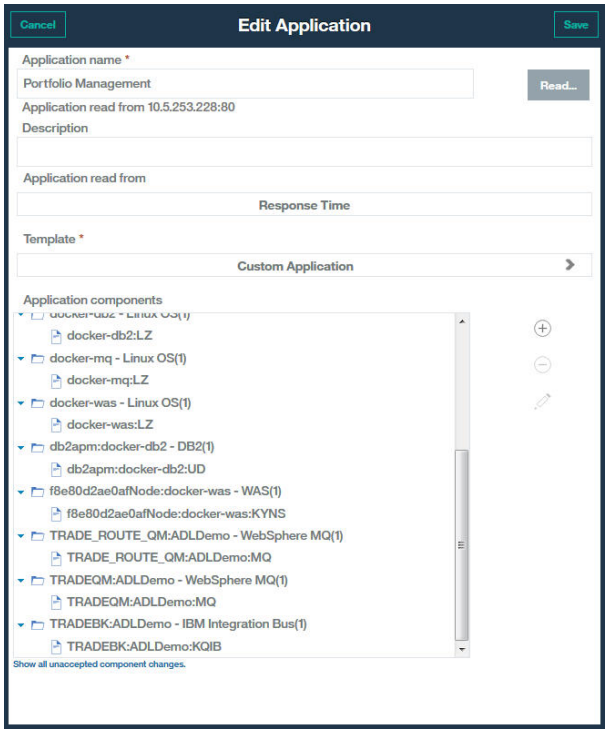
Para visualizar los componentes en Pila de integración de IBM, realice los pasos siguientes en el Application Performance Dashboard:

1. En el Application Performance Dashboard, pulse **Añadir aplicación**.



2. En la ventana **Editar aplicación**, añada un nombre de aplicación y pulse **Añadir componentes** +.
3. En la ventana **Seleccionar componente**, seleccione **IBM Integration Bus**.
4. En **Editor de componentes**, seleccione las instancias del componente necesario y pulse **Añadir**.

   Las instancias de IBM Integration Bus detectadas se añaden automáticamente a esa lista.
5. Pulse **Atrás** y repita los pasos 3 - 4 para **WebSphere MQ** y **DataPower Appliance**. Continúe añadiendo las instancias de IBM Integration Bus, IBM MQ y Dispositivo DataPower hasta que se haya completado Pila de integración de IBM.



6. Pulse **Cerrar** y a continuación **Guardar** para volver al Application Performance Dashboard.

Resultados

Consejo: Si la Topología de transacciones agregada no muestra inicialmente la topología que se espera, espere a que esta se renueve y vuélvalo a comprobar en unos minutos. Si la topología sigue sin ser lo que se espera, es posible que haya un problema en la aplicación y que esta no se comunique con los componentes esperados. Compruebe su entorno.

Visualización de los resultados de la supervisión de la Pila de integración de IBM

Puede ver los resultados de la supervisión de la Pila de integración de IBM en las topologías y páginas de middleware. Puede ver también los sucesos generados cuando una transacción infringe un umbral definido.

Acerca de esta tarea

En las topologías, puede ver las interacciones entre los componentes middleware. En la Topología de transacciones agregada y la Topología de instancia de transacciones se visualizan los nodos de middleware siguientes:

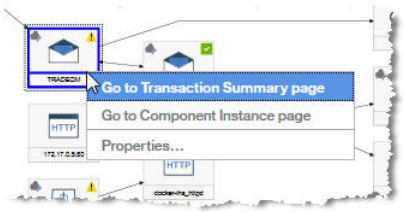
- IBM Integration Bus
- IBM MQ
- Dispositivo DataPower

Pase el cursor por encima de un nodo para mostrar una ventana de propiedades que muestra información para explicar porqué un nodo tiene un estado determinado. El estado viene determinado por las situaciones; se muestran las situaciones con un estado erróneo.

Procedimiento

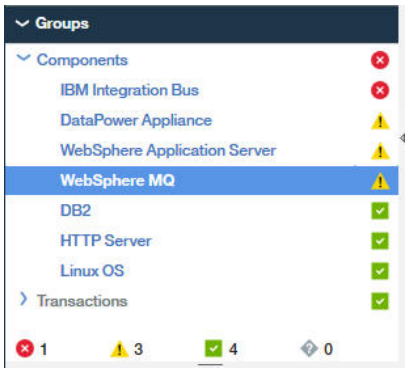
Puede enlazar de nodos de la topología a información más detallada sobre ese nodo:

1. Pulse el botón derecho (del ratón) en un nodo.



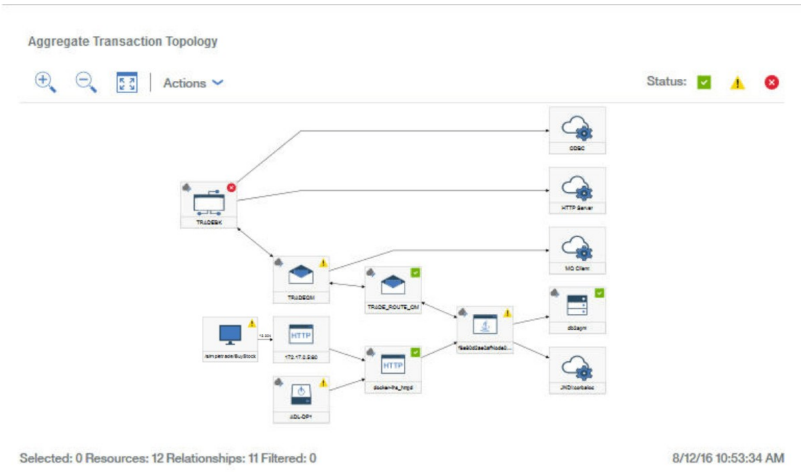
2. Seleccione **Ir a la página Componente** para mostrar información sobre el componente.
3. Seleccione **Ir a la página Resumen de transacciones** para mostrar información sobre las transacciones de middleware.

   Consejo: Seleccione **Grupos** > **Componentes** > ***componente middleware*** en el navegador y seleccione un periodo de solicitud en el widget de volumen para ir al mismo panel de instrumentos.



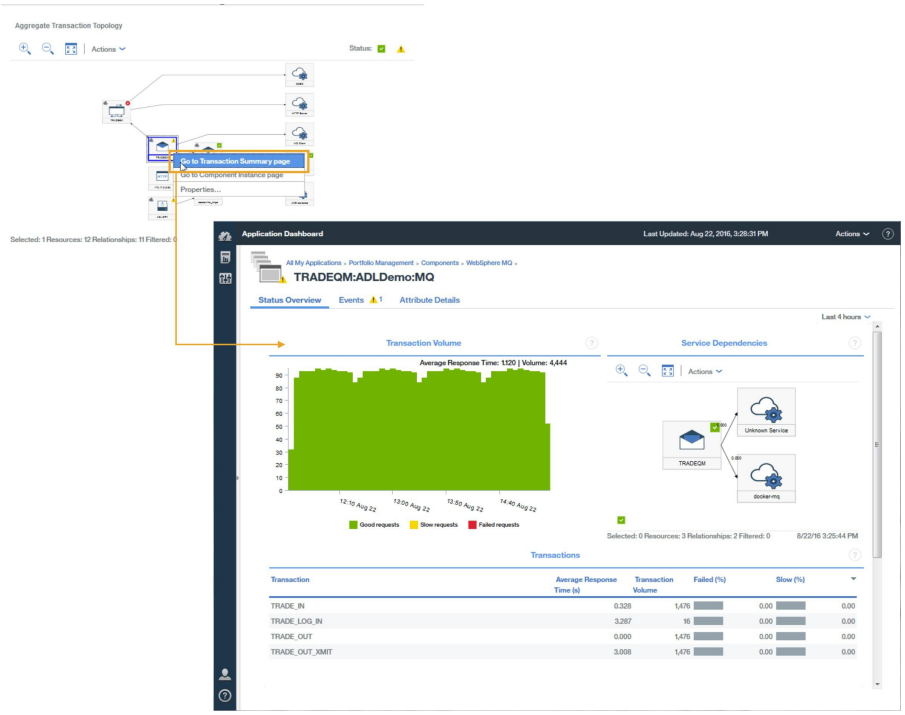
Topología de transacciones agregada

La Topología de transacciones agregada se visualiza en el panel de instrumentos Resumen de aplicaciones.



Las topologías de transacciones agregadas pueden mostrar los nodos de IBM MQ, IBM Integration Bus y Dispositivo DataPower. Obtenga mayor nivel de destalle de estos nodos para obtener más información sobre la pila de integración de middleware.

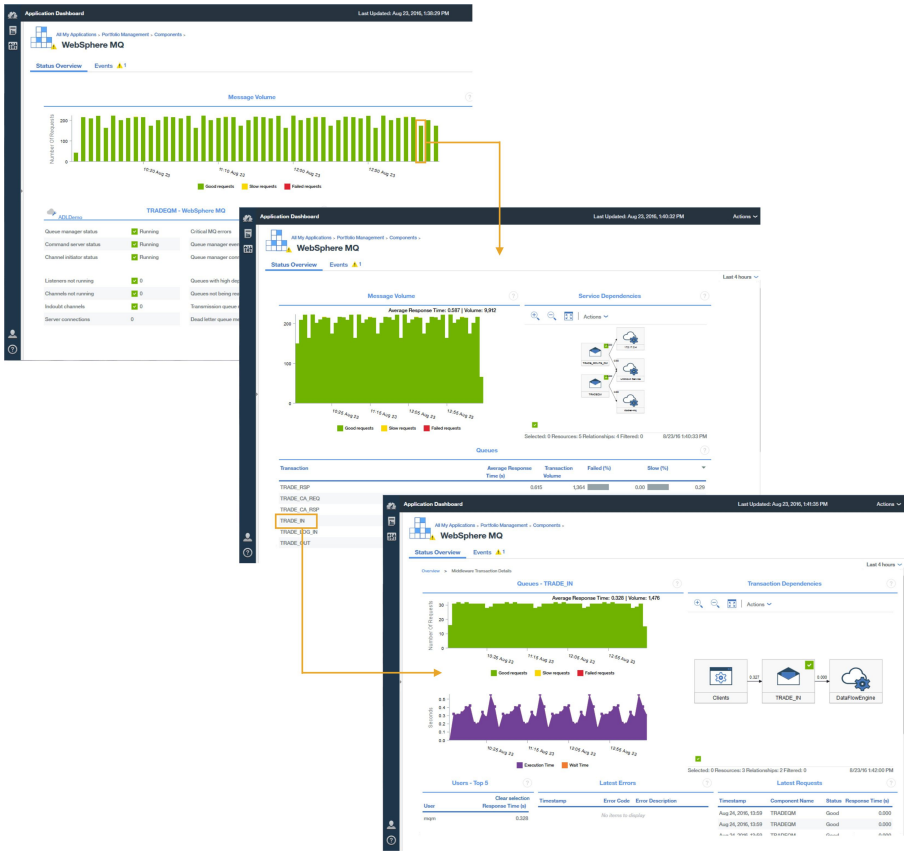
Para obtener detalles, pulse el botón derecho (del ratón) en un nodo de middleware de la topología de transacciones agregadas y seleccione **Ir a la página Resumen de transacciones**. O bien, seleccione **Grupos** > **Componentes** > ***componente middleware*** en el navegador y seleccione un periodo de solicitud en el widget de volumen para acceder a la misma información.



Detalles de transacción de middleware

En la página Resumen de transacciones de middleware, puede ver mayor nivel de detalle de la transacción de middleware.

Para ver mayor nivel de detalle de transacción de middleware para el componente, complete estos pasos:



1. En la página Resumen de transacciones de middleware para el componente, seleccione un intervalo de supervisión en el gráfico **Mensaje o volumen**.
2. En el **Resumen de transacciones de middleware**, en el widget **Colas**, **Intermediarios**, o **Dispositivos**, seleccione una cola, un intermediario o un dispositivo.

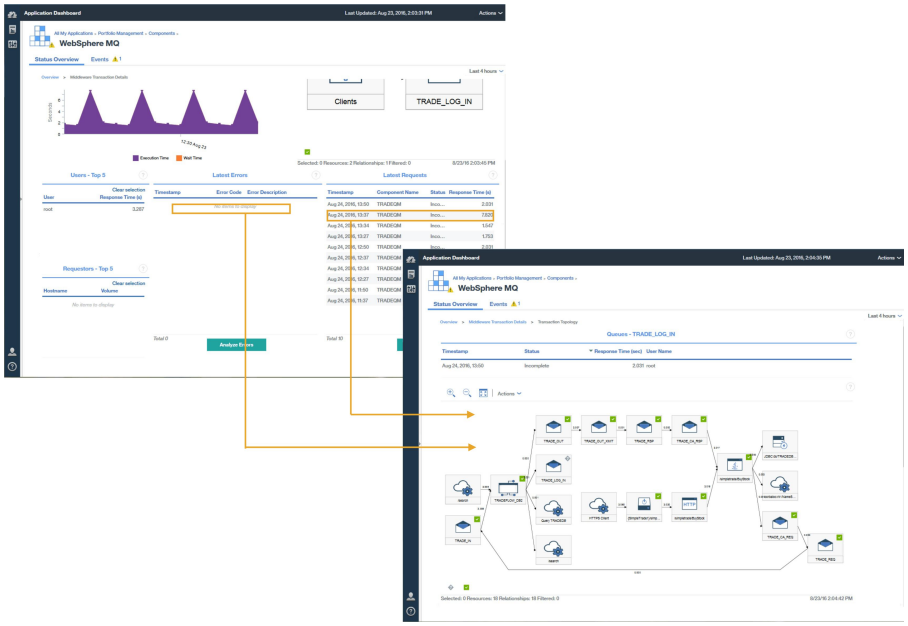
Análisis de errores e instancias

Desde la página Detalles de transacciones de middleware, puede ver más detalles de información que ayuda a analizar los errores y las instancias y a acceder a la topología de instancias de transacciones.

Para ver los detalles de errores e instancias de los componentes middleware y luego de la topología de instancias de transacciones, en la página **Detalles de transacción** realice uno de los pasos siguientes:

- Pulse **Analizar errores** para mostrar la página **Análisis de errores**, luego seleccione un error.
- Pulse **Analizar solicitudes** para mostrar la página **Análisis de instancia**, luego seleccione una instancia.

O bien, en la página **Detalles de transacción**, seleccione un error o una instancia para ir directamente a la topología de instancias de transacciones.



Las topologías de instancias de transacciones muestran los nodos de middleware siguientes:

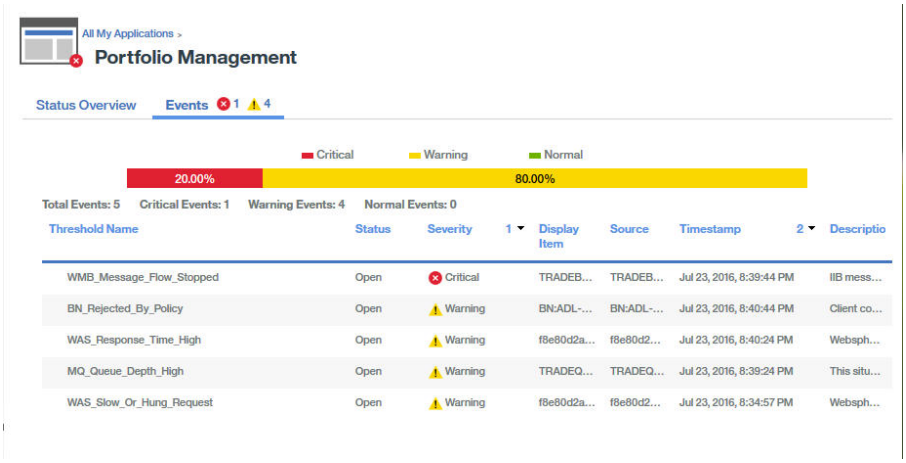
- Message Queue Manager
- Intermediarios de IBM Integration Bus
- Dispositivos DataPower

Seleccione un nodo para mostrar sus propiedades que explican porqué un nodo tiene un estado determinado.

Se mostrará una gráfica de Gantt de transacción para la cola o el intermediario seleccionados. La gráfica de Gantt ayuda a aislar los contribuidores más significativos al tiempo de respuesta global de la transacción.

Sucesos

Los umbrales de rastreo de transacciones predeterminados generan sucesos para la Pila de integración de IBM además de los otros agentes.



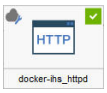
Si desea más información sobre los sucesos predeterminados del Rastreo de transacciones, consulte “Umbrales de suceso para la supervisión de transacciones ” en la página 1048.

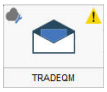
Puede añadir umbrales para crear más sucesos, por ejemplo, para las tasas de transacciones lentas o que están por debajo de un determinado umbral.

Si desea más información sobre cómo añadir sucesos, consulte “Creación de umbrales para generar sucesos para la supervisión de transacciones” en la página 1050.

Diagnóstico de problemas en su entorno
Si las instancias de transacciones para uno de los componentes de su entorno son lentas o fallan, se asigna al componente afectado un estado adecuado.

Un nodo puede tener uno de los estados siguientes:

- 

Correcto, el nodo tiene una marca rodeada de un cuadrado verde en la esquina superior derecha
- 

Aviso, el nodo tiene un signo de exclamación rodeado de un triángulo amarillo en la esquina superior derecha
- 

Crítico, el nodo tiene un fondo rojo y una cruz dentro de un círculo rojo en la esquina superior derecha

Para identificar la causa de los problemas de estos componentes con estado de aviso o crítico, pulse con el botón derecho del ratón sobre el nodo y busque la información detallada sobre cuál puede ser la causa de las anomalías.

Descarga de los agentes y recopiladores de datos

Puede acceder a la suscripción de Cloud APM desde el sitio web de IBM Marketplace. Inicie la sesión con su cuenta y descargue los archivos de archivado de instalación. Los archivos de archivado de instalación incluyen los archivos de configuración e instalación de los agentes y recopiladores de datos.

Puede aprender más sobre cómo descargar agentes y recopiladores de datos siguiendo los pasos de estas guías de aprendizaje:

- “Guía de aprendizaje: Descarga e instalación de un agente” en la página 108
- “Guía de aprendizaje: Descarga y configuración de un recopilador de datos” en la página 112

Puede registrarse para una prueba activa o una suscripción adquirida para una de las ofertas de IBM Cloud Application Performance Management desde IBM Marketplace.

IBM Marketplace

Regístrese para una prueba gratuita en IBM Marketplace > Cloud APM > Free Trial. Compre una suscripción en IBM Marketplace > Cloud APM > Purchase . Inicie la sesión en la página Productos y servicios para descargar los agentesy recopiladores de datos.

La página **Productos y servicios** está disponible para los suscriptores activos. Si tiene algún problema, vaya a Soporte de Marketplace.

Probar la conectividad

Para obtener información sobre la comprobación de conectividad con el Servidor de Cloud APM, que se utiliza para descargar paquetes, consulte Conectividad de red.

Guía de aprendizaje: Descarga e instalación de un agente

Utilice esta guía de aprendizaje para obtener una experiencia práctica de la descarga e instalación de un Agente de sistema operativo Windows de Cloud APM desde IBM Marketplace. A continuación, puede iniciar la Consola de Cloud APM y comprobar el estado del recurso supervisado visualizando los indicadores clave de rendimiento (ICR) en los paneles de instrumentos.

Acerca de esta tarea

Esta guía de aprendizaje implica descargar el paquete de instalación de Windows desde la página **Productos y servicios** de IBM Marketplace, extraer los archivos de instalación e instalar el Agente de sistema operativo Windows. Volverá a **Productos y servicios** para iniciar la Consola de Cloud APM y abrir el Panel de instrumentos del rendimiento de aplicaciones para comprobar el estado del sistema Windows.

Procedimiento

1. Si no se ha registrado en IBM Marketplace, regístrese con su IBMid y contraseña y vaya a **Productos y servicios**.

   La página **Productos y servicios** está disponible para los suscriptores activos. Si tiene algún problema, vaya al Foro de Cloud Application Performance Management o al Soporte de Marketplace.
2. Descargue el archivo de archivado de instalación de Windows:
   a) En el recuadro de suscripción de Cloud APM, pulse **Gestionar** > **Descargas**.
   b) Seleccione el sistema operativo Windows.

      Seleccione el paquete IBM Cloud Application Performance Management Agents de 64 bits. Si utiliza la versión de Windows de 32 bits, seleccione el paquete de agentes de 32 bits.
   c) Pulse **Descargar** y guarde el archivo de archivado de instalación del agente en el sistema. Ejemplo:

      ```
      C:\Users\MY_ADMIN\Downloads\IAPM_Agent_Install.zip
      ```
3. En el sistema Windows local, vaya al directorio donde ha guardado el archivo de archivado descargado y extráigalo.
   Por ejemplo, en el Explorador de Windows, abra el directorio **Descargas**, pulse `IAPM_Agent_Install.zip` con el botón derecho del ratón y seleccione **Extraer todo**.
4. Abra un indicador de mandatos como administrador:
   a) En el menú **Inicio** de Windows, escriba `comando` en el cuadro de búsqueda.
   b) Pulse el botón derecho (del ratón) en el **Símbolo del sistema** en la lista que se muestra y seleccione **Ejecutar como administrador**.
5. Cambie al directorio donde ha extraído los archivos de instalación.

Ejemplo:

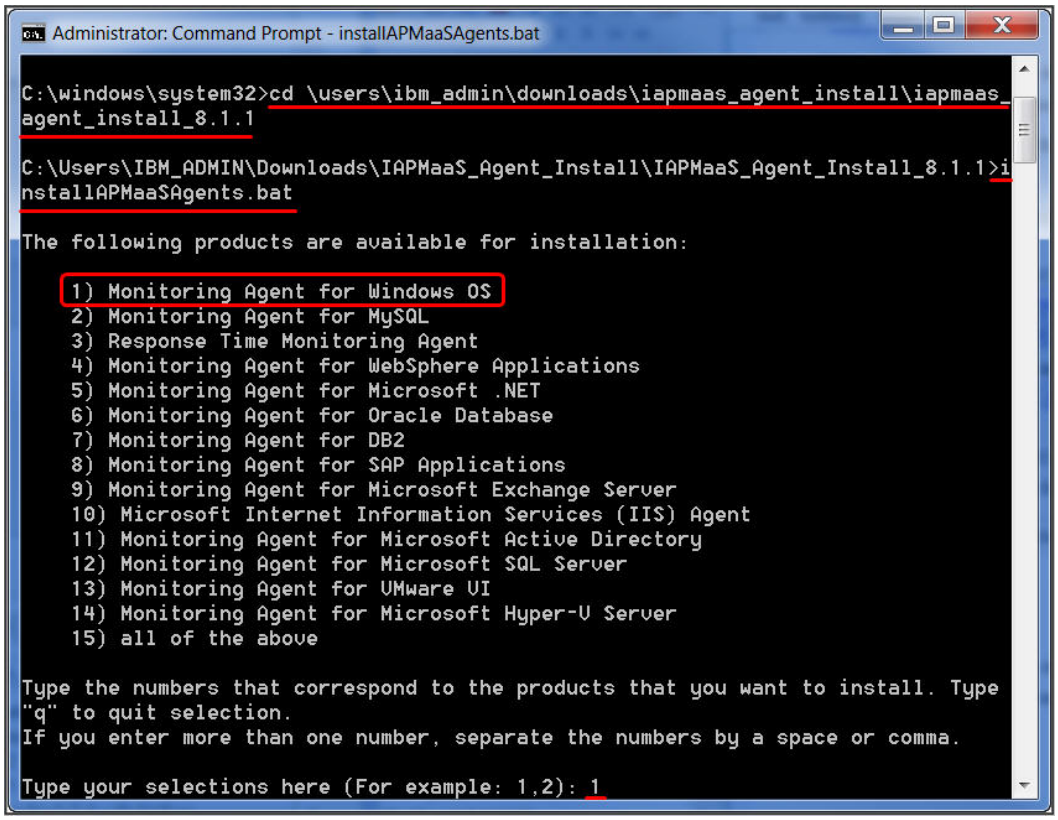
```
cd C:\Users\MY_ADMIN\Downloads\IAPM_Agent_Install\IAPM_Agent_Install_8.1.4
```

6. Ejecute el script de instalación para instalar el Agente de sistema operativo Windows:
   a) Especifique el mandato siguiente:

   ```
   installAPMAgents.bat
   ```

   b) En la lista de agentes disponibles, especifique el número que corresponde al Agente de sistema operativo Windows.
   c) Responda a las solicitudes para confirmar que desea instalar el Agente de sistema operativo Windows y para aceptar el acuerdo de licencia.

   Se inicia una exploración de requisitos previos de su entorno y tarda varios minutos en completarse. Si faltan algunos requisitos, recibirá un mensaje que le dirigirá a un archivo de registro que contiene la causa del error. Un requisito previo como insuficiente espacio de disco, detendrá la instalación. Debe resolver la anomalía y volver a iniciar el script de instalación. Si tiene algún problema, vaya al Foro de Cloud Application Performance Management o envíe un correo electrónico `ainfo@ibmserviceengage.com`.



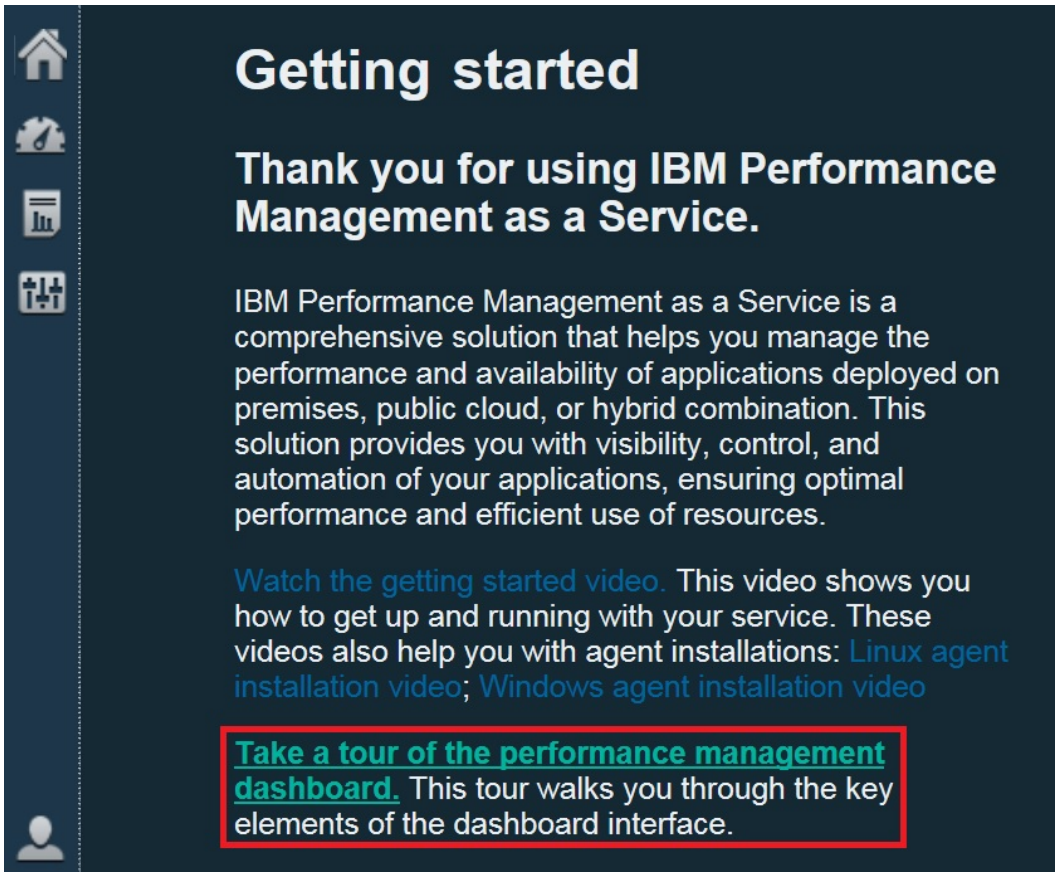
Para ver el informe de requisitos del sistema operativo Windows, consulte System requirements (APM Developer Center).

Después de la instalación satisfactoria, el Agente de sistema operativo Windows se inicia automáticamente y puede iniciar la Consola de Cloud APM para empezar a supervisar el sistema Windows.

Nota: Si el entorno incluye un cortafuegos que no permite las conexiones HTTPS salientes transparentes a un host externo, debe configurar un proxy directo para las comunicaciones entre el agente y Servidor de Cloud APM. El proxy de reenvío permite reenviar todo el tráfico a un punto específico en la red y luego permite solo una conexión única a través del cortafuegos. Para obtener más información, consulte “Configuración de agentes para la comunicación mediante un proxy directo” en la página 165.

7. Vuelva a **Productos y servicios** en IBM Marketplace y pulse **Iniciar** desde el recuadro de suscripción de Cloud APM.

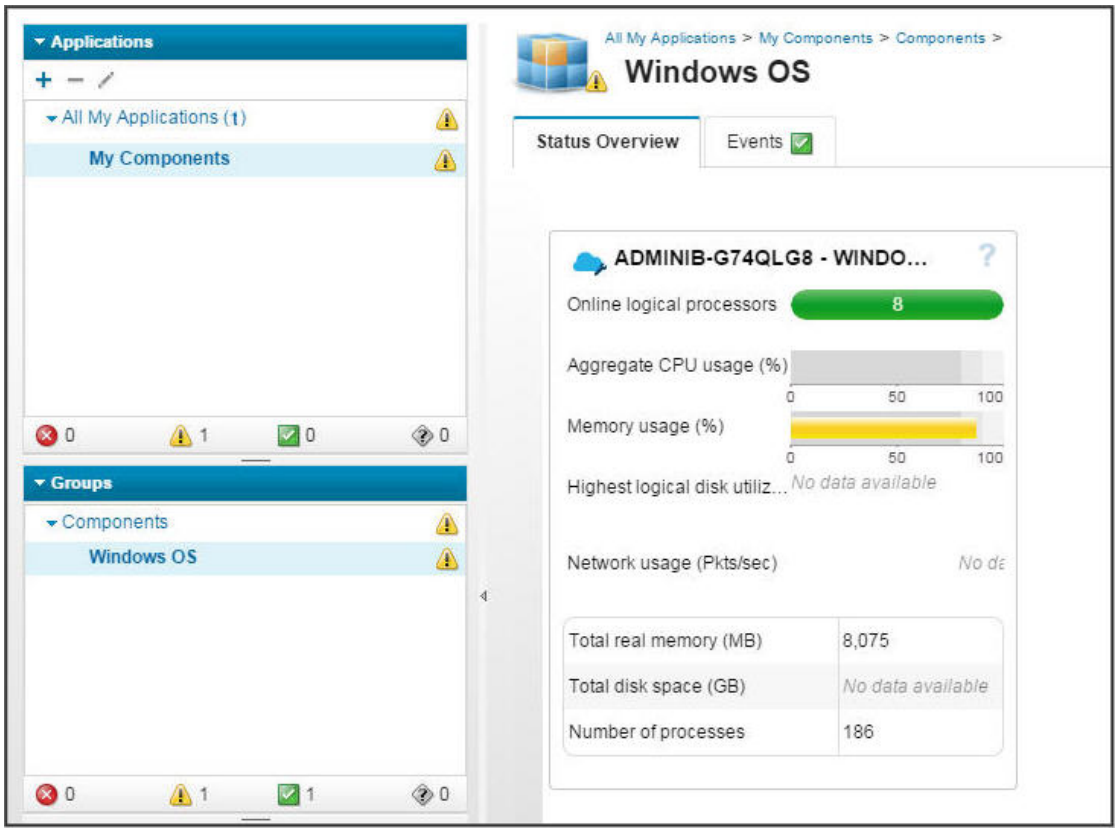
   Se abrirá la Consola de Cloud APM en la página **Cómo empezar** donde puede obtener información sobre las características, ver vídeos para distintos escenarios de usuarios y abrir las páginas de la consola asociadas.
8. En la página **Cómo empezar**, pulse "Visita guiada por el panel de herramientas de gestión de rendimiento" para realizar una visita rápida por los elementos de navegación.



9. Abra el panel de instrumentos de resumen del sistema operativo Windows:
   a) En la barra de navegación, pulse **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones**.
      - Se mostrará el panel de instrumentos **Todas mis aplicaciones** con un recuadro de estado de resumen para cada aplicación definida en el entorno. Inicialmente, solo se muestra la aplicación predefinida **Mis componentes**.
      - Si aparece la ventana **Añadir aplicación** en lugar de **Mis componentes**, cree una aplicación para ver el recurso supervisado:
        1) Especifique un nombre para la aplicación, como "Mis aplicaciones".
        2) Pulse +.
        3) Desplácese hasta el final de la lista **Seleccione el componente** y pulse **SO Windows**.
        4) En el editor de componentes, pulse `Primario:`*`nombre_host`*`:NT`, pulse **Añadir** y pulse **Atrás** para añadir el agente a la aplicación.
        5) Pulse **Guardar** para cerrar la ventana y ver un recuadro de estado de resumen para la nueva aplicación en el panel de instrumentos.
   b) En el recuadro de resumen, pulse **Componentes**.
      - Se mostrará el panel de instrumentos de resumen para el sistema gestionado del SO Windows. Desde aquí, puede pulsar en cualquier lugar del widget de grupo de resumen de estado para ver

un mayor nivel de detalle de los paneles de instrumentos detallados con ICR notificados desde el Agente de sistema operativo Windows.

- Puede tardar unos minutos que el agente recién iniciado se comunique con la infraestructura de supervisión y envíe los ICR a la consola.



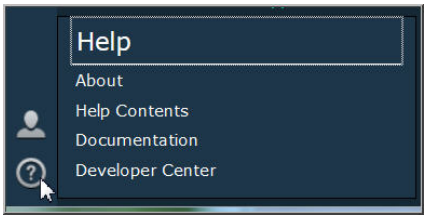
Si el agente no se comunica con el Servidor de Cloud APM o no se inicia, el panel de instrumentos de resumen no muestra ningún ICR y el estado se muestra como desconocido. Puede utilizar el mandato **os-agent** para comprobar el estado e iniciar el agente si es necesario. Abra un indicador de mandatos como administrador y especifique el mandato **os-agent status** desde la carpeta `C:\IBM\APM\bin`. Si el agente no se ha iniciado, especifique el mandato **os-agent start**.

Resultados

Ha instalado un agente de Cloud APM y ha observado los datos de supervisión enviados a los Panel de instrumentos del rendimiento de aplicaciones.

Qué hacer a continuación

- Explore la consola: mientras utiliza la Consola de Cloud APM, explore las características. Puede obtener información sobre el panel de instrumentos actual pulsando en el banner de ventana. Puede abrir el sistema de ayuda o la colección de temas de Cloud APM en IBM Knowledge Center desde el menú **Ayuda** de la barra de navegación.



- Instale otros agentes: tiene todos los archivos de instalación necesarios para instalar otros tipos de agentes de Windows para supervisar el entorno. Puede instalar también los agentes en otros sistemas del entorno. Si tiene sistemas AIX o Linux, descargue el archivo de archivado de instalación asociado.

Algunos tipos de agente tienen requisitos previos que se deben completar antes de instalarlos y la mayoría de los tipos de agente requieren alguna configuración después de instalarlos. Para obtener más información, consulte la “Preinstalación en sistemas AIX” en la página 127, la “Preinstalación en sistemas Linux” en la página 134, la “Preinstalación en sistemas Windows” en la página 142 y la Capítulo 7, “Configuración del entorno”, en la página 165.

Guía de aprendizaje: Descarga y configuración de un recopilador de datos

Utilice esta guía de aprendizaje para obtener una experiencia práctica de la descarga y configuración de un recopilador de datos de Bluemix Ruby de Cloud APM desde IBM Marketplace. A continuación, puede iniciar la Consola de Cloud APM y comprobar el estado del recurso supervisado visualizando los indicadores clave de rendimiento (ICR) en los paneles de instrumentos.

Acerca de esta tarea

Esta guía de aprendizaje, implica la descarga del paquete del recopilador de datos para aplicaciones Bluemix de la página **Productos y servicios** de IBM Marketplace, la extracción de los archivos de configuración y la configuración del recopilador de datos de Bluemix Ruby en un sistema Linux. Volverá a **Productos y servicios** para iniciar la Consola de Cloud APM y abrir el Panel de instrumentos del rendimiento de aplicaciones para comprobar el estado de salud de la aplicación Bluemix Ruby.

Procedimiento

1. Si no se ha registrado en IBM Marketplace, regístrese con su IBMid y contraseña y vaya a **Productos y servicios**.

   La página **Productos y servicios** está disponible para los suscriptores activos. Si tiene algún problema, vaya al Foro de Cloud Application Performance Management o al Soporte de Marketplace.
2. Descargue el paquete de recopiladores de datos para aplicaciones Bluemix `IBM_Bluemix_Data_Collectors_Install.tgz`.
3. En el sistema local, vaya al directorio donde ha guardado el archivo de archivado descargado y extráigalo ejecutando el mandato siguiente:

   ```
   tar -zxvf IBM_Bluemix_Data_Collectors_Install.tgz
   ```

   Obtendrá cuatro archivos comprimidos, cada uno de los cuales representa un recopilador de datos para un tipo de aplicación Bluemix. El paquete de recopilador de datos para aplicaciones Bluemix Ruby es `ruby_datacollector.tgz`.
4. Extraiga los archivos de `ruby_datacollector.tgz` ejecutando el mandato siguiente, por ejemplo:

   ```
   tar -zxvf ruby_datacollector.tgz
   ```

   Obtendrá una carpeta `ibm_ruby_dc`.
5. Copie toda la carpeta `etc` de `ibm_ruby_dc` en la carpeta raíz de la aplicación Ruby ejecutando el mandato siguiente, por ejemplo:

   ```
   cp –r directorio a la carpeta etc  directorio de inicio de la aplicación Ruby
   ```

   Si extrae el recopilador de datos en el directorio `/opt/ibm/ccm/ibm_ruby_dc/etc` y el directorio de inicio de la aplicación Ruby es `/root/ruby_app/`, el mandato será el siguiente:

   ```
   cp –r /opt/ibm/ccm/ibm_ruby_dc/etc /root/ruby_app/
   ```
6. Añada la sección siguiente a `Gemfile` en la carpeta de inicio de la aplicación Bluemix Ruby:

   ```
   gem 'logger',  '>= 1.2.8'
   source 'https://managemserver.ng.bluemix.net' do
     gem 'ibm_resource_monitor'
     gem 'stacktracer'
   end
   ```
7. Ejecute el mandato `bundle lock` para volver a generar el archivo `Gemfile.lock`.

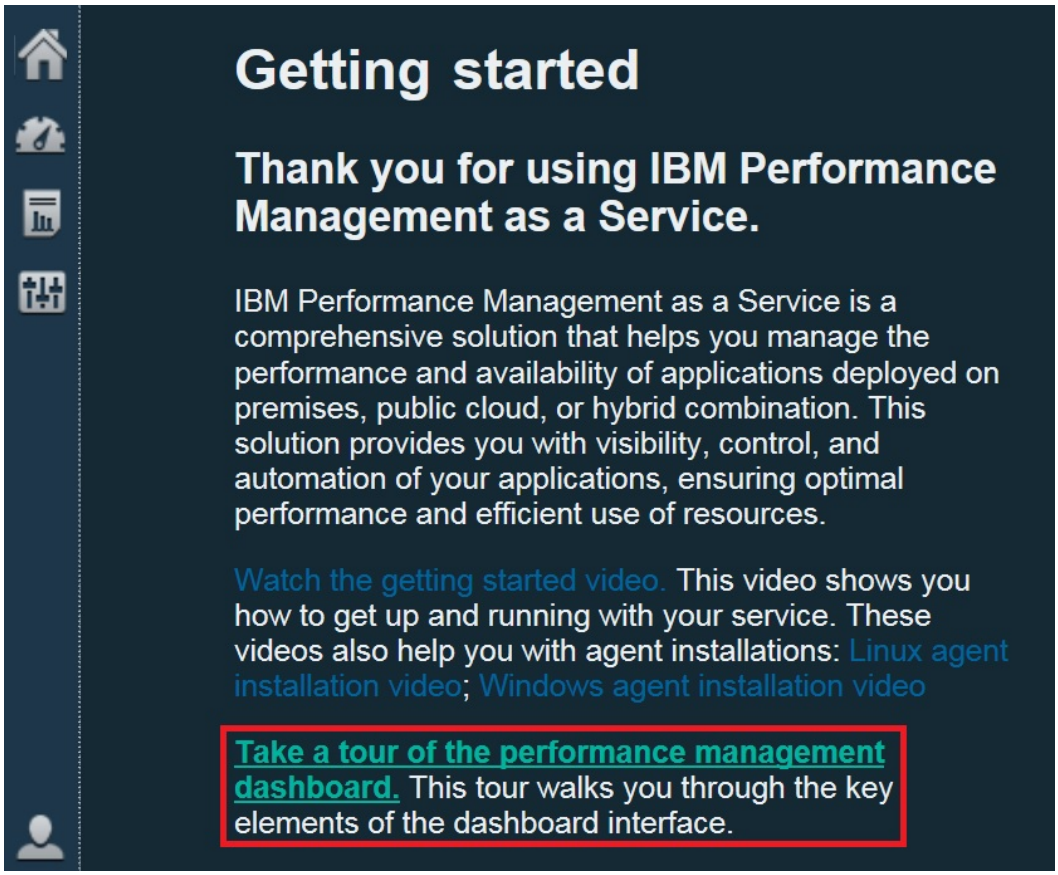
8. Desde el directorio de inicio de la aplicación Ruby, ejecute el mandato siguiente:

```
cf push
```

9. Vuelva a **Productos y servicios** en IBM Marketplace y pulse **Iniciar** desde el recuadro de suscripción de Cloud APM.

   Se abrirá la Consola de Cloud APM en la página **Cómo empezar** donde puede obtener información sobre las características, ver vídeos para distintos escenarios de usuarios y abrir las páginas de la consola asociadas.

10. En la página **Cómo empezar**, pulse "Visita guiada por el panel de herramientas de gestión de rendimiento" para realizar una visita rápida por los elementos de navegación.



11. Abra el panel de instrumentos de resumen de aplicaciones Bluemix Ruby:

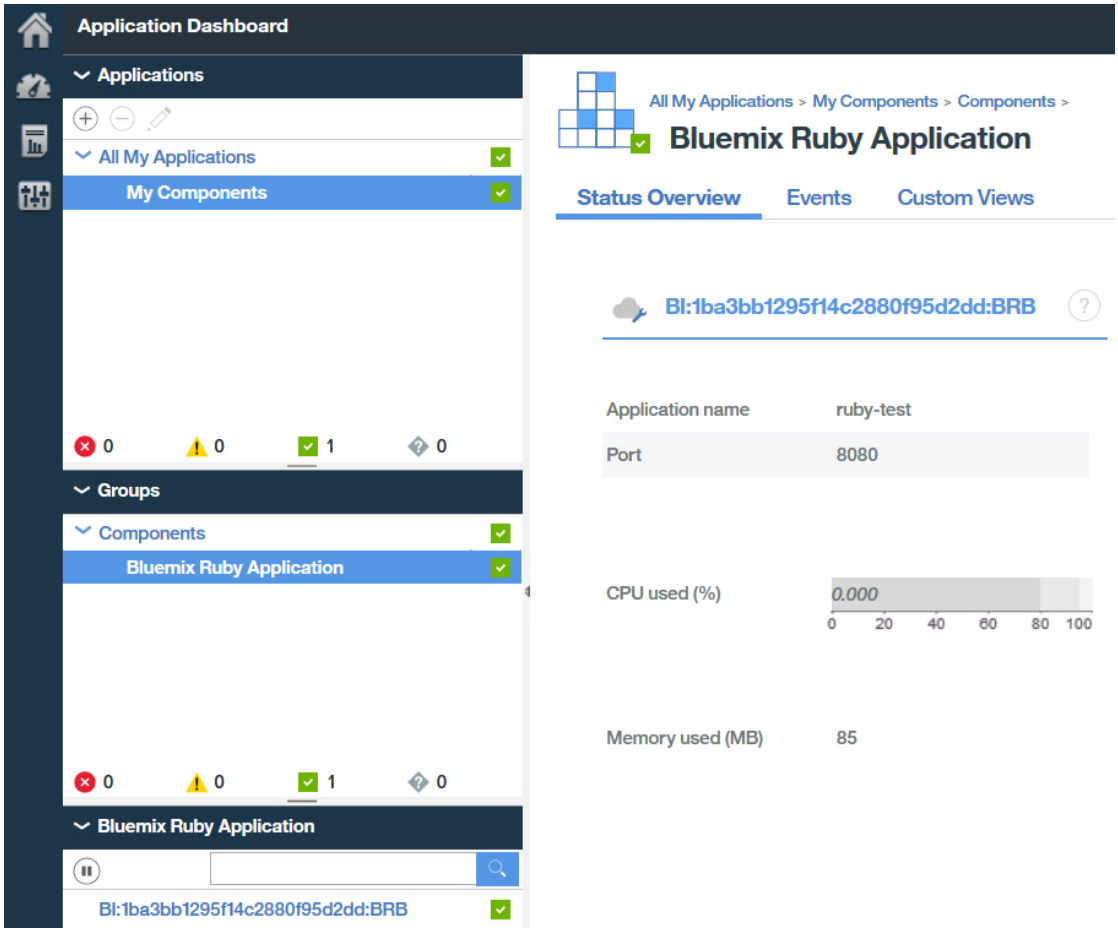
    a) En la barra de navegación, pulse **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones**.

    - Se mostrará el panel de instrumentos **Todas mis aplicaciones** con un recuadro de estado de resumen para cada aplicación definida en el entorno. Inicialmente, solo se muestra la aplicación predefinida **Mis componentes**.
    - Si aparece la ventana **Añadir aplicación** en lugar de **Mis componentes**, cree una aplicación para ver el recurso supervisado:

      1) Especifique un nombre para la aplicación, como "Mis aplicaciones".
      2) Pulse +.
      3) Pulse **Aplicación Bluemix Ruby**.
      4) En el editor de componentes, seleccione una instancia, pulse **Añadir** y pulse **Atrás** para añadir el recopilador de datos a la aplicación.
      5) Pulse **Guardar** para cerrar la ventana y ver un recuadro de estado de resumen para la nueva aplicación en el panel de instrumentos.

b) En el recuadro de resumen, pulse **Componentes**.

- Se mostrará el panel de instrumentos de resumen de la aplicación Bluemix Ruby. Desde aquí, puede pulsar en cualquier lugar del widget de grupo de resumen de estado para ver un mayor nivel de detalle de los paneles de instrumentos detallados con ICR notificados desde el recopilador de datos de Bluemix Ruby.
- El recopilador de datos recién iniciado puede tardar unos minutos en comunicarse con la infraestructura de supervisión y enviar los ICR a la consola.

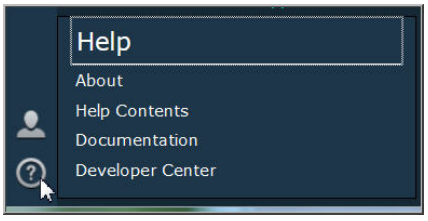


Resultados

Ha instalado un recopilador de datos de Cloud APM y ha observado los datos de supervisión enviados a los Panel de instrumentos del rendimiento de aplicaciones.

Qué hacer a continuación

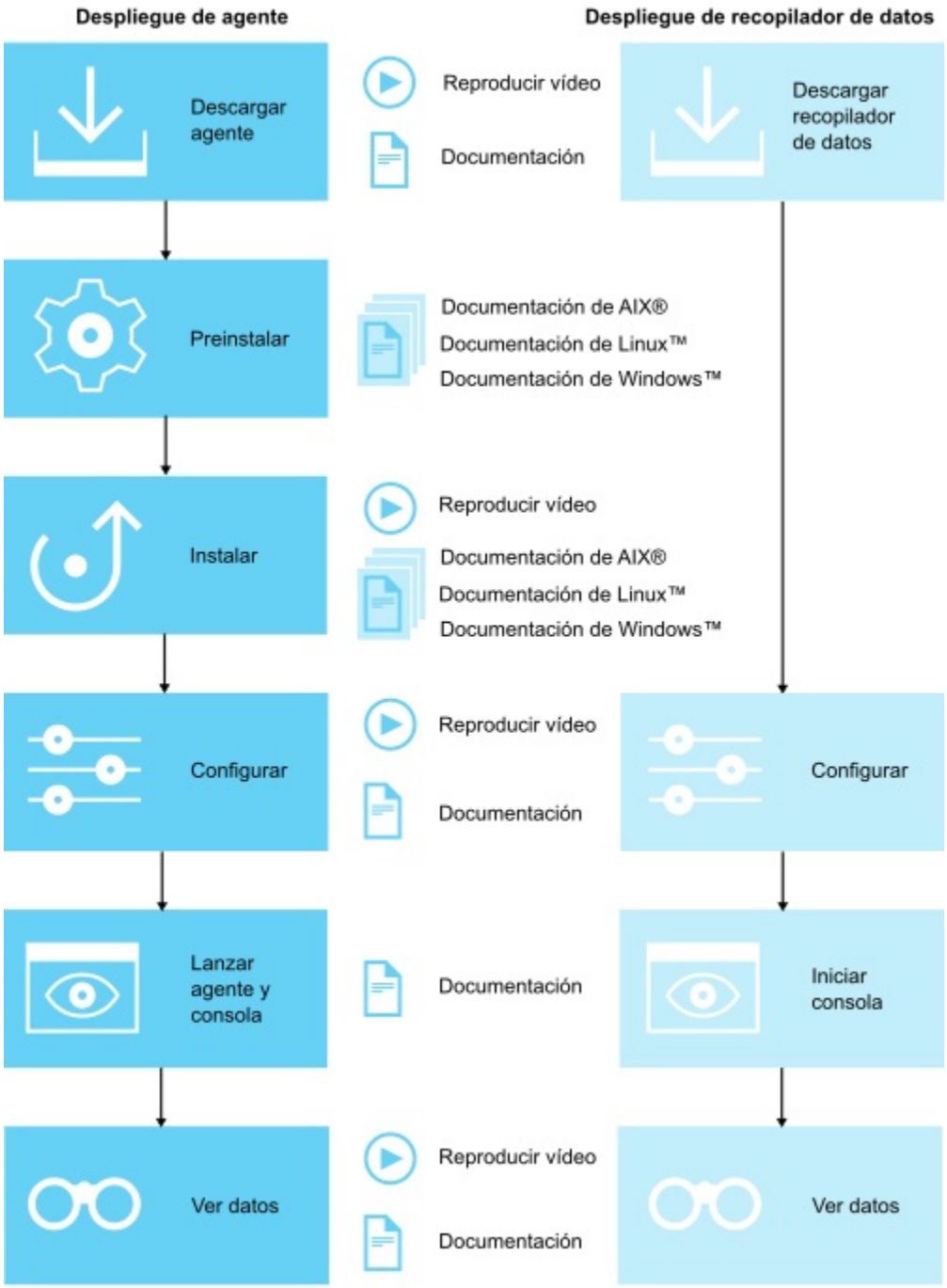
- Explore la consola: mientras utiliza la Consola de Cloud APM, explore las características. Puede obtener información sobre el panel de instrumentos actual pulsando en el banner de ventana. Puede abrir el sistema de ayuda o la colección de temas de Cloud APM en IBM Knowledge Center desde el menú **Ayuda** de la barra de navegación.



- Instale otros recopiladores de datos: tiene todos los archivos de instalación necesarios para instalar otros tipos de recopiladores de datos para supervisar el entorno. También puede instalar los recopiladores de datos en otros sistemas del entorno. Para obtener más información, consulte Capítulo 7, “Configuración del entorno”, en la página 165.

Capítulo 5. Despliegue de agentes y recopiladores de datos

Los agentes varían en las tareas necesarias entre instalación y visualización de los datos que recopilan. Algunas tareas son automáticas y otras manuales. Después de descargar los recopiladores de datos, debe configurar manualmente cada uno de ellos.



1. Reproducir vídeo de descarga

2. Descargar documentación
3. Documentación de preinstalación de AIX
4. Documentación de preinstalación de Linux
5. Documentación de preinstalación de Windows
6. Reproducir vídeo de instalación
7. Documentación de instalación de AIX
8. Documentación de instalación de Linux
9. Documentación de instalación de Windows
10. Reproducir vídeos de configuración
11. Documentación de configuración
12. Documentación de lanzamiento
13. Reproducir vídeo de vista de datos
14. Documentación de características

1. Reproducir vídeo de descarga
2. Descargar documentación
3. Documentación de preinstalación de AIX
4. Documentación de preinstalación de Linux
5. Documentación de preinstalación de Windows
6. Reproducir vídeo de instalación
7. Documentación de instalación de AIX
8. Documentación de instalación de Linux
9. Documentación de instalación de Windows
10. Reproducir vídeos de configuración
11. Documentación de configuración
12. Documentación de lanzamiento
13. Reproducir vídeo de vista de datos
14. Documentación de características

Tras la instalación, algunos agentes se configuran e inician automáticamente
Para cualquier agente iniciado, el agente se configura con los valores predeterminados. Para determinar qué agentes se configuran e inician manualmente, consulte Tabla 7 en la página 119.

Tras la instalación, algunos agentes requieren configuración manual, pero se inician automáticamente
Si desea más información sobre cómo configurar los agentes, consulte Capítulo 7, “Configuración del entorno”, en la página 165 para determinar qué agentes se configuran manualmente y se inician automáticamente, consulte Tabla 7 en la página 119.

Tras la instalación, algunos agentes se deben configurar e iniciar manualmente
Para los agentes que no se inicien automáticamente, primero deberá configurar el agente para poderlo iniciar. Para determinar qué agentes se configuran e inician manualmente, consulte Tabla 7 en la página 119.

Varios agentes de instancia requieren crear una primera instancia e iniciarse manualmente
Deberá crear la primera instancia e iniciar el agente manualmente. Un agente de varias instancias significa que una instalación única del agente crea una instancia de supervisión única para cada instancia de aplicación única. Estas instancias se visualizan en la Consola de Cloud APM como resultado. Para determinar qué agentes son de varias instancias, consulte Tabla 7 en la página 119.

Supervisión de agentes de SO y archivo de registro

Agente de sistema operativo Linux, Agente de sistema operativo UNIX y Agente de sistema operativo Windows se configuran e inician automáticamente. Sin embargo, puede configurar la supervisión de archivos de registro para los agentes de sistema operativo, de forma que pueda supervisar los archivos de registro de la aplicación. Para obtener más información, consulte "Configuración de la supervisión de archivos de registro del agente de sistema operativo" en la página 656.

Despliegue de agentes y configuración de recopilador de datos, inicio y características de instancia

Tabla 7. Lista de comprobación posterior a la instalación

Despliegue de agentes o recopilador de datos	Configurado e iniciado automáticamente	Configurado manualmente e iniciado automáticamente	Configurado e iniciado manualmente	Varias instancias (iniciadas manualmente)
Agente de Amazon EC2	—	—	—	✓
Agente de Amazon ELB	—	—	—	✓
Agente de Azure Compute	—	—	—	✓
Agente de Cassandra	—	—	✓	✓
Agente de Cisco UCS	—	—	✓	✓
Agente de Citrix VDI	—	—	—	✓
Agente de DataPower	—	—	—	✓
Agente de DataStage	—	—	✓	✓
Agente de Db2	—	—	—	✓
Agente de Hadoop	—	—	✓	—
Agente de HMC Base	—	—	—	✓
Agente de HTTP Server	✓ Debe revisar el archivo de configuración que el agente crea para el servidor HTTP. A continuación, debe añadir la configuración del recopilador de datos manualmente en el archivo de configuración del servidor.	—	—	—
Agente de IBM Cloud	—	—	—	✓
Agente de IBM Integration Bus	—	—	—	✓
Recopilador de datos de J2SE	—	✓	—	—
Agente de JBoss	—	—	—	✓

Tabla 7. Lista de comprobación posterior a la instalación (continuación)

Despliegue de agentes o recopilador de datos	Configurado e iniciado automáticamente	Configurado manualmente e iniciado automáticamente	Configurado e iniciado manualmente	Varias instancias (iniciadas manualmente)
Recopilador de datos de Liberty	—	✓	—	—
Agente de Linux KVM	—	—	✓	✓
Agente de sistema operativo Linux	✓	—	—	—
Agente de Microsoft Active Directory	—	✓ Este agente se inicia automáticamente. Sin embargo, debe configurar el agente para ver datos para algunos atributos.	—	—
Agente de Microsoft Cluster Server	—	—	✓	—
Agente de Microsoft Exchange Server	—	✓ Este agente se inicia automáticamente. Sin embargo, debe configurar el agente para ver datos para todos los atributos.	—	—
Agente de Microsoft Hyper-V Server	✓	—	—	—
Agente de Microsoft IIS	✓	—	—	—
Agente de Skype for Business Server (anteriormente conocido como agente de Microsoft Lync Server)	✓	✓ Este agente se inicia automáticamente. Sin embargo, debe configurar el agente para ver datos para algunos atributos.	—	—
Agente de Microsoft Office 365	—	—	✓	—

Tabla 7. Lista de comprobación posterior a la instalación (continuación)

Despliegue de agentes o recopilador de datos	Configurado e iniciado automáticamente	Configurado manualmente e iniciado automáticamente	Configurado e iniciado manualmente	Varias instancias (iniciadas manualmente)
Agente de Microsoft .NET	—	✓ El recopilador de datos debe estar configurado antes de que se notifiquen los datos.	—	—
Agente de Microsoft SharePoint Server	✓	—	—	—
Agente de Microsoft SQL Server	—	—	—	✓ Cada instancia de agente se debe configurar e iniciar manualmente.
Agente de MQ Appliance	—	—	—	✓
Agente de MongoDB	—	—	—	✓
Agente de MySQL	—	—	—	✓
Agente de NetApp Storage	—	—	✓	✓
Agente de Node.js	—	✓ El agente debe estar configurado antes de que se notifiquen los datos. Debe añadir un plug-in de supervisión a la aplicación Node.js.	—	—
Recopilador de datos de Node.js	—	✓	—	—
Agente de OpenStack	—	—	✓	✓
Agente de Oracle Database	—	—	—	✓
Agente de PHP	—	—	—	✓
Agente de PostgreSQL	—	—	—	✓
Recopilador de datos de Python	—	✓	—	—

Tabla 7. Lista de comprobación posterior a la instalación (continuación)

Despliegue de agentes o recopilador de datos	Configurado e iniciado automáticamente	Configurado manualmente e iniciado automáticamente	Configurado e iniciado manualmente	Varias instancias (iniciadas manualmente)
Agente de RabbitMQ	—	—	✓	✓
Agente de Supervisión de tiempo de respuesta	✓	—	—	—
Agente de Ruby	—	—	—	✓ Para diagnósticos en profundidad, el agente debe estar configurado antes de que se notifiquen los datos. Para habilitar los paneles de instrumentos de diagnóstico, debe instalar y configurar el recopilador de datos de diagnóstico.
Recopilador de datos de Ruby	—	✓	—	—
Agente de SAP	—	—	✓	✓
Agente de SAP HANA Database	—	—	✓	✓
Agente de SAP NetWeaver Java Stack	—	—	✓	✓
Agente de Siebel	—	—	—	✓
Agente de Sterling Connect Direct	—	—	—	✓
Agente de Sterling File Gateway	—	—	✓	✓
Agente de Sybase	—	—	✓	✓

Tabla 7. Lista de comprobación posterior a la instalación (continuación)

Despliegue de agentes o recopilador de datos	Configurado e iniciado automáticamente	Configurado manualmente e iniciado automáticamente	Configurado e iniciado manualmente	Varias instancias (iniciadas manualmente)
Agente de Synthetic Playback	✓ El agente se configura e inicia automáticamente para aplicaciones públicas, de cara al exterior, pero las transacciones deben crearse en el Gestor de scripts sintéticos antes de que se informe de los datos.	✓ El agente se inicia automáticamente pero el agente debe configurarse para aplicaciones privadas e internas. Las transacciones se deben crear en el Gestor de scripts sintéticos antes de que se informe de los datos.	—	✓
Agente de Tomcat	—	—	—	✓
Agente de sistema operativo UNIX	✓	—	—	—
Agente de VMware VI	—	—	✓	✓
Agente de WebLogic	—	—	—	✓
Agente de WebSphere Applications	—	✓ El agente se inicia automáticamente pero el recopilador de datos debe estar configurado antes de que se notifiquen los datos.	—	—
Agente de WebSphere Infrastructure Manager	—	—	—	✓
Agente de WebSphere MQ	—	—	—	✓
Agente de sistema operativo Windows	✓	—	—	—

Capítulo 6. Instalación de los agentes

IBM instala y gestiona la infraestructura de IBM Cloud Application Performance Management. Para supervisar las aplicaciones, seleccione e instale los agentes de supervisión para las aplicaciones que quiere supervisar. Puede instalar los agentes en los sistemas operativos Linux, AIX o Windows. Los recopiladores de datos autónomos no requieren instalación.

Si elige recopiladores de datos autónomos para supervisar las aplicaciones, puede omitir el procedimiento de instalación. Continúe en Capítulo 7, “Configuración del entorno”, en la página 165 para obtener instrucciones sobre cómo desplegar recopiladores de datos para supervisar las aplicaciones.

Supervisión remota

Algunos agentes pueden instalarse de forma remota con respecto al recurso que están supervisando. Los agentes siguientes admiten la supervisión remota:

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for DataPower - Este agente sólo puede instalarse en una máquina remota.
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HMC Base
- Monitoring Agent for IBM Cloud
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for JBoss - Si desea utilizar este agente para la supervisión de recursos, instálelo remotamente o localmente. Si desea utilizar el agente para el rastreo de transacciones y diagnósticos en profundidad, instálelo localmente.
- Monitoring Agent for Linux KVM
- Monitoring Agent for MariaDB
- Monitoring Agent for Microsoft Cluster Server
- Monitoring Agent for Microsoft Exchange Server
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent for Microsoft SharePoint Server
- Monitoring Agent for MongoDB
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for OpenStack
- Monitoring Agent for Oracle Database
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database

- Monitoring Agent for SAP NetWeaver Java Stack - Si desea utilizar este agente para la supervisión de recursos, instálelo remotamente o localmente. Si desea utilizar el agente para el rastreo de transacciones y diagnósticos en profundidad, instálelo localmente.
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic - Si desea utilizar este agente para la supervisión de recursos, instálelo remotamente o localmente. Si desea utilizar el agente para el rastreo de transacciones y diagnósticos en profundidad, instálelo localmente.
- Agente de Supervisión de tiempo de respuesta - Si está utilizando el componente analizador de paquetes, el agente puede instalarse de forma remota o local. Si está utilizando el módulo Tiempo de respuesta de IBM HTTP Server, el agente debe estar instalado en la misma máquina que el servidor HTTP.

Instalación de agentes en sistemas UNIX

Instale agentes de supervisión en los sistemas AIX o Solaris para los recursos que desee gestionar.

Lista de agentes que puede instalar en AIX

- Monitoring Agent for DataPower
- Monitoring Agent for Cassandra
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HMC Base
- Monitoring Agent for HTTP Server
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for MQ Appliance
- Monitoring Agent for Oracle Database
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sybase Server
- Monitoring Agent for UNIX OS
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ
- Agente de Supervisión de tiempo de respuesta

Lista de agentes que puede instalar en Solaris Sparc

- Monitoring Agent for Db2
- Monitoring Agent for HTTP Server
- Monitoring Agent for JBoss
- Monitoring Agent for MySQL
- Monitoring Agent for Oracle Database
- Monitoring Agent for SAP Applications

- Monitoring Agent for Sybase Server
- Monitoring Agent for UNIX OS
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebLogic

Lista de agentes que puede instalar en Solaris X86

- Monitoring Agent for Db2
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for SAP Applications
- Monitoring Agent for Sybase Server
- Monitoring Agent for UNIX OS
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

Preinstalación en sistemas AIX

Debe llevar a cabo las tareas de preinstalación necesarias antes de instalar los agentes en los sistemas AIX. Algunas tareas de preinstalación son específicas del agente y otras tareas se aplican a varios agentes.

Nota: Estos requisitos son adicionales a los requisitos identificados en los Informes de compatibilidad de productos de software.

Para conocer los requisitos de versión actuales y las dependencias del agente, consulte System requirements (APM Developer Center) para obtener un enlace a los informes de compatibilidad de productos de software.

Todos los agentes

Las tarea de preinstalación siguientes son aplicables a todos los agentes:

Probar la conectividad
Antes de instalar los agentes, asegúrese de que el sistema puede comunicarse con el Servidor de Cloud APM. Para obtener información sobre la comprobación de conectividad con el Servidor de Cloud APM, consulte Conectividad de red.

Instalación de usuario no root
Debe tener permisos de lectura, grabación y ejecución sobre el directorio de instalación. De lo contrario se cancela la instalación. Para obtener más información sobre la instalación de usuario no root, consulte “Instalación de agentes como usuarios no root” en la página 146.

Limitación de 70 caracteres para la vía de acceso de instalación
El directorio de instalación y la vía de acceso no deben tener más de 70 caracteres.

Limitación de 100 caracteres para los nombres de archivo `.tar`
El mandato **`tar`** predeterminado en sistemas AIX no puede manejar nombres de archivos mayores de 100 caracteres. Para evitar problemas de instalación, realice los pasos siguientes:

1. Descargue e instale la versión GNU del mandato **`tar`** desde el sitio web AIX Toolbox for Linux Applications.
2. Haga que la versión GNU sea el mandato **`tar`** predeterminado. Complete uno de los pasos siguientes:
   - Añada `/opt/freeware/bin` al principio de la variable de entorno *PATH* actual. Por ejemplo:

     ```
     export PATH=/opt/freeware/bin:$PATH
     ```

     donde /opt/freeware/bin es el directorio de bin de GUN.

- Sustituya `/bin/tar` por un enlace simbólico a `/opt/freeware/bin/tar` como se indica a continuación:

```
ln -s /opt/freeware/bin/tar /bin/tar
```

De forma alternativa, actualice a la última versión de AIX para recibir el arreglo de código para manejar nombres de archivo de más de 100 caracteres. Para obtener detalles, consulte la Nota técnica del mandato TAR para AIX V6.1 o la Nota técnica del mandato TAR para AIX V7.1.

Establecimiento de la variable de entorno *CANDLEHOME*

Si previamente utilizó ITM Agent Converter para instalar y configurar un agente en el mismo sistema gestionado, la variable de entorno *CANDLEHOME* ha cambiado a ese directorio en el que instaló el agente con Agent Converter. Antes de instalar y configurar un agente Cloud APM nativo, debe establecer la variable de entorno *CANDLEHOME* en un directorio diferente, de lo contrario, el agente Cloud APM no se puede iniciar.

Agentes específicos

Las tareas de preinstalación siguientes son aplicables a los agentes especificados:

Agente de DataPower

Antes de que se instale el agente, el comprobador de requisitos comprueba que *ulimit* está establecido en **unlimited** en AIX. Debe ejecutar el mandato **ulimit -d unlimited** para asegurarse de que la variable de entorno del sistema *max data segment size* está establecida en **unlimited**. Este agente no puede instalarse en la misma máquina que el dispositivo DataPower que desea supervisar.

Agente de HMC Base

Si planea instalar el agente como un usuario root, debe asegurarse de que el sistema TL07 esté instalado. Si planea instalar el agente como un usuario no root, debe asegurarse de que el sistema TL08 esté instalado solo para AIX versión 6.

Agente de HTTP Server

Instale y ejecute este agente como usuario root. Utilice el mismo ID de usuario para instalar y ejecutar el agente. Si instala y ejecuta el agente como usuario no root, este último debe tener el mismo ID de usuario que el que ha iniciado el IBM HTTP Server. De lo contrario, el agente tendrá problemas para descubrir el IBM HTTP Server.

La instalación falla en AIX porque en el sistema AIX, el mandato **.tar** predeterminado ha truncado una vía de acceso larga. Si desea más información, consulte la sección "Limitación de 100 caracteres para los nombres de archivo `.tar`" en este tema.

AIX solo: instale el programa de utilidad lynx o la aplicación curl.

Agente de Oracle Database

En Red Hat Enterprise Linux versión 5 y versión 6 y SUSE Linux Enterprise Server versión 11 y versión 12 x64, si el Agente de Oracle Database supervisa la base de datos Oracle de forma remota, debe instalar primero los clientes instantáneos de Oracle. Instale los clientes instantáneos de Oracle desde Oracle Technology Network - Instant Client Downloads.

el cliente instantáneo v10.x, v11.x y v12.x están soportados en el Agente de Oracle Database.

Agente de Supervisión de tiempo de respuesta

Antes de instalar el Agente de Supervisión de tiempo de respuesta, revise la sección de planificación de la instalación aquí: “Planificación de la instalación ” en la página 712.

Agente de SAP HANA Database

1. Instale el cliente HDBSQL del cliente de base de datos SAP HANA versión 1.00.102.06 o posterior en el sistema AIX.
2. Ejecute el mandato siguiente para añadir la vía de acceso del directorio de instalación a la variable de entorno **LIBPATH**:

   `export LIBPATH=$LIBPATH:`*`vía_acceso_directorio_instalación`*

Ejemplo: `export LIBPATH=$LIBPATH:/usr/sap/hdbclient`, donde `/usr/sap/hdbclient` es la vía de instalación del cliente de base de datos SAP HANA.

Importante:

Si la vía de instalación del cliente de base de datos SAP HANA no se añade a la variable de entorno **LIBPATH**, el explorador de requisitos previos devuelve el resultado `FAIL`.

La variable de entorno que ha añadido mediante el mandato de exportación, sólo se conserva para la sesión concreta del terminal. Por lo tanto, asegúrese de que ejecuta el script de instalación del agente en el mismo terminal que ha utilizado para añadir la variable de entorno.

Agente de WebSphere Applications
Antes de que se instale el agente, el comprobador de requisitos comprueba que *ulimit* está establecido en **524000** en el sistema AIX. Debe ejecutar el mandato **`ulimit -d 524000`** para asegurarse de que la variable de entorno del sistema *max data segment size* está establecida en **524000**.

Preinstalación en sistemas Solaris

Debe llevar a cabo las tareas de preinstalación necesarias antes de instalar los agentes en sistemas Solaris. Algunas tareas de preinstalación son específicas del agente y otras tareas se aplican a varios agentes.

Nota: Estos requisitos son adicionales a los requisitos identificados en los Informes de compatibilidad de productos de software.

Para conocer los requisitos de versión actuales y las dependencias del agente, consulte System requirements (APM Developer Center) para obtener un enlace a los informes de compatibilidad de productos de software.

Todos los agentes

Las tarea de preinstalación siguientes son aplicables a todos los agentes:

Probar la conectividad
Antes de instalar los agentes, asegúrese de que el sistema puede comunicarse con el Servidor de Cloud APM. Para obtener información sobre la comprobación de conectividad con el Servidor de Cloud APM, consulte Conectividad de red.

Instalación de usuario no root
Debe tener permisos de lectura, grabación y ejecución sobre el directorio de instalación. De lo contrario se cancela la instalación. Para obtener más información sobre la instalación de usuario no root, consulte “Instalación de agentes como usuarios no root” en la página 146.

Limitación de 70 caracteres para la vía de acceso de instalación
El directorio de instalación y la vía de acceso no deben tener más de 70 caracteres.

Limitación de 100 caracteres para los nombres de archivo `.tar`
El mandato **`tar`** predeterminado en sistemas Solaris no puede manejar los nombres de archivo que tienen más de 100 caracteres. Para evitar errores de tipo @LongLink, siga estos pasos:

1. Descargue e instale la versión GNU del mandato **`tar`** desde el sitio web http://www.gnu.org.
2. Haga que la versión GNU sea el mandato **`tar`** predeterminado. Complete uno de los pasos siguientes:
   - En la variable de entorno *PATH*, ponga la siguiente variable primero:

     ```
     export PATH=/opt/freeware/bin:$PATH
     ```

   - Sustituya `/bin/tar` por el enlace simbólico a `/opt/freeware/bin/tar`

Establecimiento de la variable de entorno *CANDLEHOME*
Si previamente utilizó ITM Agent Converter para instalar y configurar un agente en el mismo sistema gestionado, la variable de entorno *CANDLEHOME* ha cambiado a ese directorio en el que instaló el agente con Agent Converter. Antes de instalar y configurar un agente Cloud APM nativo, debe

establecer la variable de entorno *CANDLEHOME* en un directorio diferente, de lo contrario, el agente Cloud APM no se puede iniciar.

Agentes específicos

Las tareas de preinstalación siguientes son aplicables a los agentes especificados:

Agente de HTTP Server
Instale y ejecute este agente como usuario root. Utilice el mismo ID de usuario para instalar y ejecutar el agente. Si instala y ejecuta el agente como usuario no root, este último debe tener el mismo ID de usuario que el que ha iniciado el IBM HTTP Server. De lo contrario, el agente tendrá problemas para descubrir el IBM HTTP Server.

Instalación de agentes

Puede instalar cualquier combinación de agentes de supervisión en un sistema gestionado. Por ejemplo, si instala el Agente de Ruby para supervisar las aplicaciones de Ruby On Rails, quizá prefiera instalar también el Agente de Supervisión de tiempo de respuesta, el Agente de sistema operativo Linux o los dos agentes. Con el Agente de Supervisión de tiempo de respuesta, puede recopilar más información de tiempo de respuesta de las aplicaciones de Ruby. Con el Agente de sistema operativo Linux, puede supervisar otros aspectos del sistema, como la CPU global, la memoria y el disco.

La oferta determina qué agentes de supervisión están disponibles para la instalación. Si desea una lista de los agentes incluidos en cada oferta, consulte "Capacidades" en la página 54.

Para obtener una lista de los agentes que se ejecutan en los sistemas AIX y Solaris, consulte "Instalación de agentes en sistemas UNIX" en la página 126.

Antes de empezar

Descargue los agentes. Consulte "Descarga de los agentes y recopiladores de datos" en la página 107.

Revise la información de "Requisitos del sistema" en la página 87 para asegurarse de que cumple los requisitos para los agentes que planea instalar.

Revise las tareas previas a la instalación antes de instalar los agentes.

- Para los sistemas AIX, consulte el "Preinstalación en sistemas AIX" en la página 127.
- Para los sistemas Solaris, consulte "Preinstalación en sistemas Solaris" en la página 129.

Importante: Java Runtime solo se instala cuando el agente lo necesita y no siempre está disponible. Además, ksh ya no es necesario para la instalación del agente y se da soporte a SELinux en modalidad de imposición.

Acerca de esta tarea

Puede instalar los agentes de supervisión como un usuario root o no root. Si no tiene privilegios de usuario root y desea instalar un agente de supervisión, puede instalar el agente como usuario no root, consulte "Instalación de agentes como usuarios no root" en la página 146. Además, puede instalar el agente como usuario no root si es administrador del sistema principal y no desea ejecutar el agente de supervisión como usuario root. El flujo de instalación es el mismo que para un usuario root.

Se da soporte a la coexistencia de agentes. Puede instalar agentes de IBM Cloud Application Performance Management en el mismo sistema donde están instalados los agentes de IBM Tivoli Monitoring. Sin embargo, ambos tipos de agente no se pueden instalar en el mismo directorio. Para obtener más información sobre la coexistencia de agentes, consulte "Coexistencia del agente de Cloud APM y el agente de Tivoli Monitoring" en la página 984.

Procedimiento

1. Abra una sesión en el shell de terminal en el sistema AIX o Solaris.
2. En el sistema, navegue al directorio donde ha descargado el archivo .tar.

Los agentes deben estar instalados en el sistema donde esté instalada la aplicación que desea supervisar. Si es necesario, transfiera el archivo de archivado de instalación al sistema para que se pueda supervisar. El archivo de archivado contiene el script de instalación y el de agente.

Recuerde: Asegúrese de que el directorio no contiene una versión más antigua del archivo de archivado.

3. Extraiga los archivos de instalación de utilizando el mandato siguiente:

```
tar -xf ./archivos de instalación
```

donde *archivos_instalación* es el nombre del archivo de instalación correspondiente a su oferta.

El script de instalación se extrae en un directorio especificado para el archivo de archivado y la versión. Por ejemplo: *oferta*_Agent_Install_8.1.4.0. El archivo binario del agente y los archivos relacionados con la configuración se extraen en los subdirectorios dentro de este directorio.

4. Opcional: Este paso SÓLO es necesario para Solaris 10. Debe crear un enlace dinámico a ksh antes de ejecutar el script de instalación en Solaris 10.
   a) Realice una copia de seguridad del mandato /bin/sh:

```
mv /bin/sh /bin/sh.bkup_origin
```

   b) Cree un enlace dinámico al mandato ksh:

```
ln -s /bin/ksh /bin/sh
```

   c) Confirme que el resultado apunta a ksh:

```
ls -l /bin/sh
```

5. Ejecute el script de instalación desde el directorio que se llama para el archivo de archivado y la versión:

```
./installAPMAgents.sh
```

Para instalar los agentes en modalidad silenciosa, consulte "Instalación silenciosa de agentes" en la página 149.

6. Especifique si desea instalar agentes individuales, una combinación de los agentes o todos los agentes.
7. En función de si está instalando o actualizando los agentes, realice uno de los pasos siguientes:
   - Si está instalando los agentes, especifique el directorio de inicio de instalación del agente o utilice el directorio predeterminado aplicable:
     – /opt/ibm/apm/agent
   - Si está actualizando los agentes, después de que se le solicite el directorio de inicio de instalación de los agentes, especifique el directorio de instalación de la versión anterior de los agentes.
8. Cuando se le pregunte si acepta el acuerdo de licencia, entre 1 para aceptar el acuerdo y continuar, o entre 2 para rechazarlo.

   Tras entrar 1 (aceptar), se inicia una exploración de requisitos previos del entorno y tarda unos pocos minutos en completarse. Si faltan algunos requisitos, un mensaje le dirigirá a un archivo de registro que contiene la causa del error. Un requisito previo como la falta de una biblioteca o espacio de disco insuficiente detendrá la instalación. Debe resolver la anomalía y volver a iniciar el script de instalación.
9. Si ha instalado los agentes mediante un ID de usuario no root, debe actualizar los scripts de arranque del sistema (consulte "Instalación de agentes como usuarios no root" en la página 146).
10. Cuando se haya completado la instalación y la línea de mandatos esté disponible, puede repetir los pasos de este procedimiento para instalar más agentes de supervisión en el sistema gestionado.

Qué hacer a continuación

Configure el agente como sea necesario. Si el agente de supervisión requiere configuración como se describe en Capítulo 5, “Despliegue de agentes y recopiladores de datos”, en la página 117 o si desea revisar los valores predeterminados, consulte Capítulo 7, “Configuración del entorno”, en la página 165.

- Si utiliza un proxy directo porque el cortafuegos no permite conexiones HTTPS salientes transparentes a hosts externos, debe editar el archivo de configuración de entorno del agente. Para obtener instrucciones, consulte “Configuración de agentes para la comunicación mediante un proxy directo” en la página 165.
- Si ha actualizado un agente desde una versión anterior, identifique cualquier tarea de reconfiguración o migración que debe completar antes de iniciar sesión en la Consola de Cloud APM. Para obtener información sobre esas tareas, consulte “Actualización de los agentes” en la página 1173. Después de una actualización, debe reiniciar todos los agentes que el instalador no configura e inicia automáticamente.

Para iniciar un agente, ejecute el mandato siguiente:

```
./nombre-agent.sh start
```

Para obtener información sobre los mandatos de agente de supervisión, incluido el *nombre* que se va a utilizar, consulte “Utilización de mandatos de agente” en la página 184. Si desea información sobre qué agentes se inician de forma automática y manual, consulte Capítulo 5, “Despliegue de agentes y recopiladores de datos”, en la página 117.

Después de una actualización, debe reiniciar todos los agentes que el instalador no configura e inicia automáticamente.

Después de configurar e iniciar el agente, vea los datos que el agente está recopilando.

- Si no ha iniciado sesión, siga las instrucciones en “Inicio de la Consola de Cloud APM” en la página 1009.
- Si desea ver sistemas gestionados del dominio de IBM Tivoli Monitoring en los Panel de instrumentos del rendimiento de aplicaciones, complete las tareas descritas en “Integración con IBM Tivoli Monitoring V6.3 ” en la página 983.

Instalación de agentes en sistemas Linux

Instale agentes de supervisión en los sistemas Linux para los recursos que desea gestionar.

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for DataPower
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HTTP Server
- Monitoring Agent for IBM Cloud
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Internet Services
- Monitoring Agent for MQ Appliance
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for JBoss

- Monitoring Agent for Linux OS
- Monitoring Agent for Linux KVM
- Monitoring Agent for MariaDB
- Monitoring Agent for Microsoft SQL Server
- Monitoring Agent for MongoDB
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for Node.js
- Monitoring Agent for OpenStack
- Monitoring Agent for Oracle Database
- Monitoring Agent for PHP
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for Ruby
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for Sybase Server
- Monitoring Agent for Synthetic Playback
- Monitoring Agent for Tomcat
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere Infrastructure Manager
- Monitoring Agent for WebSphere MQ
- Agente de Supervisión de tiempo de respuesta

Los agentes siguientes están soportados en sistemas Linux on Power Little Endian (pLinux LE):

- Monitoring Agent for Db2
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Linux OS
- Monitoring Agent for Tomcat - Soporte disponible para la supervisión de recursos.
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

Los agentes siguientes están soportados en sistemas Linux for System z:

- Monitoring Agent for Db2
- Monitoring Agent for HTTP Server - El rastreo de transacciones no está soportado.
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Linux OS
- Agente de Supervisión de tiempo de respuesta
- Monitoring Agent for Tomcat

- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

El agente siguiente está soportado en sistemas Linux for System x:

- Monitoring Agent for HTTP Server - El rastreo de transacciones no está soportado.

Preinstalación en sistemas Linux

Debe llevar a cabo las tareas de preinstalación necesarias antes de instalar los agentes en los sistemas Linux. Algunas tareas de preinstalación son específicas del agente y otras tareas se aplican a varios agentes.

Nota: Estos requisitos son adicionales a los requisitos identificados en los Informes de compatibilidad de productos de software.

Para conocer los requisitos de versión actuales y las dependencias del agente, consulte System requirements (APM Developer Center) para obtener un enlace a los informes de compatibilidad de productos de software.

Todos los agentes

Las tarea de preinstalación siguientes son aplicables a todos los agentes:

Probar la conectividad
Antes de instalar los agentes, asegúrese de que el sistema puede comunicarse con el Servidor de Cloud APM. Para obtener información sobre la comprobación de conectividad con el Servidor de Cloud APM, consulte Conectividad de red.

Instalación de usuario no root
Debe tener permisos de lectura, grabación y ejecución sobre el directorio de instalación. De lo contrario se cancela la instalación. Para obtener más información sobre la instalación de usuario no root, consulte “Instalación de agentes como usuarios no root” en la página 146.

Limitación de 70 caracteres para la vía de acceso de instalación
El directorio de instalación y la vía de acceso no deben tener más de 70 caracteres.

Establecimiento de la variable de entorno *CANDLEHOME*
Si previamente utilizó ITM Agent Converter para instalar y configurar un agente en el mismo sistema gestionado, la variable de entorno *CANDLEHOME* ha cambiado a ese directorio en el que instaló el agente con Agent Converter. Antes de instalar y configurar un agente Cloud APM nativo, debe establecer la variable de entorno *CANDLEHOME* en un directorio diferente, de lo contrario, el agente Cloud APM no se puede iniciar.

Sistemas operativos específicos

Red Hat Enterprise Linux (RHEL) 8

El paquete libnsl.so.1 es necesario en RHEL 8

De forma predeterminada, `libnsl.so.1` no se instala en Red Hat Enterprise Linux release 8.0. Sin este paquete, ningún agente puede instalarse correctamente. Pida a su administrador que configure un repositorio yum y ejecute este mandato:

```
yum install libnsl
```

Cuando la instalación se haya realizado correctamente, podrá ver `/usr/lib64/libnsl.so.1`.

Nota: El paquete `libnsl.so.1` sólo es necesario para los agentes. No es necesario que realice este paso para los recopiladores de datos.

Eludir el escáner de requisitos previos para algunos agentes

Antes de actualizar el escáner de requisitos previos para que sea compatible con los requisitos más recientes, para algunos agentes, puede eludir el escáner de requisitos previos. Para conocer

los escenarios adecuados e instrucciones, consulte "Eludir la exploración de requisitos previos" en la página 150.

Nota: No es necesario que realice este paso para los recopiladores de datos.

Agentes específicos

Las tareas de preinstalación siguientes son aplicables a los agentes especificados:

Agente de DataPower

Debe ejecutar el mandato **ulimit -d unlimited** para asegurarse de que la variable de entorno del sistema *max data segment size* está establecida en **unlimited**. Este agente no puede instalarse en la misma máquina que el dispositivo DataPower que desea supervisar.

Agente de DataStage

1. Habilite los parámetros en el archivo DSODBConfig.cfg. Complete los pasos siguientes:
   a. Abra el archivo DSODBConfig.cfg en la ubicación siguiente de un editor:

      dir_instalación_infosphere_information_server/Server/DSODB

   b. Descomente los parámetros siguientes eliminado el símbolo #:

      MonitorLinks=1
      JobRunUsage=1
      ResourceMonitor=1
      DSODBON=1

   c. Edite los valores de estos parámetros igual que 1.
2. Copie el controlador JDBC de la base de datos que se utiliza para la configuración del repositorio de metadatos en el sistema agente.
   a. JDBC 4 tipo 4 o posterior. Ejemplo: db2jcc4.jar
   b. Controlador JDBC tipo 4 para Oracle. Ejemplo: ojdbc6.jar
   c. Controlador JDBC para MS SQL:
      - Sqljdbc41.jar requiere un JRE de 7 y da soporte a la API de JDBC 4.1.
      - Sqljdbc42.jar requiere un JRE de 8 y da soporte a la API de JDBC 4.2.

Agente de HTTP Server

Si instala este agente como un usuario root, debe utilizar el mismo ID de usuario para ejecutar y configurar el agente.

Si instala y ejecuta el agente como un usuario no root, el usuario no root debe tener el mismo ID de usuario que el que ha iniciado el IBM HTTP Server. De lo contrario, el agente tendrá problemas para descubrir el IBM HTTP Server. Puede utilizar el mismo ID de usuario para ejecutar y configurar el agente.

Agente de Linux KVM

El Monitoring Agent for Linux KVM es un agente multiinstancia y multiconexión, y da soporte a conexiones con el hipervisor KVM basado en Enterprise Linux y los entornos Red Hat Enterprise Virtualization Manager (RHEV-M). Puede crear varias instancias de este agente para supervisar varios hipervisores en un entorno de hipervisor de RHEV-M o KVM. Puede supervisar cargas de trabajo virtualizadas y analizar la capacidad de recursos entre varias máquinas virtuales. Para conectar el agente a una máquina virtual en el entorno de hipervisor KVM, debe instalar los requisitos previos: libvirt*.rpm y Korn Shell Interpreter (pdksh). El agente recopila medidas conectando remotamente a un hipervisor libvirt que gestiona las máquinas virtuales.

Agente de Microsoft SQL Server

Para supervisar un entorno de Microsoft SQL, el controlador ODBC de Microsoft SQL Server y Microsoft SQL debe estar instalado antes de instalar Monitoring Agent for Microsoft SQL Server. Por ejemplo, para instalar el controlador ODBC en Red Hat Enterprise Linux, utilice el siguiente mandato:

```
sudo yum install unixODBC
sudo yum install msodbcsql17
```

Para completar la ejecución del comprobador de requisitos previos, el agente debe configurarse en el arreglo temporal 15 del servidor de Cloud Application Performance Management Versión 8.1.4.0 (8.1.4.0-IBM-APM-SERVER-IF0015.tar) o posterior.

Agente de MongoDB

Debe instalar y configurar el Agente de MongoDB en el sistema donde está instalado el servidor de bases de datos MongoDB.

Agente de MySQL

Para supervisar un entorno MySQL, el servidor MySQL y el controlador JDBC MySQL debe estar instalado antes de instalar el Monitoring Agent for MySQL. Por ejemplo, para instalar el controlador JDBC en Red Hat Enterprise Linux, utilice el mandato siguiente:

```
yum install mysql-connector-java
```

Después de iniciar la instalación del agente y durante la comprobación de requisitos previos del nombre de paquete MySQL, recibirá un aviso si se utiliza un proveedor que no sea Red Hat, como por ejemplo Oracle. Si el servidor MySQL y el controlador JDBC están disponibles, el aviso no hace que la instalación falle y puede pasar por alto el mensaje. Salida de ejemplo:

```
Escenario: Exploración de requisitos previos
KSE - Comprobador de requisitos previos de Monitoring Agent for MySQL [versión 01000005]:
Propiedad                    Result Encontrado  Esperado
========                     ====== =====       ========
os.package.mysql-server        WARN  Unavailable  mysql-server-5.1.12+
os.package.mysql-connector-java WARN Unavailable mysql-connector-java-5.
1.12+
```

Agente de Node.js

la versión de Node.js que utilice para ejecutar la aplicación supervisada debe ser la misma que la versión instalada de forma predeterminada.

Actualmente Node.js v5 no está soportado.

Agente de OpenStack

Para poder utilizar Agente de OpenStack, debe tener el software siguiente en el servidor en el que instala el agente:

- Python 2.6.0 o posterior, o Python 2.7.0 o posterior
- Clientes OpenStack más recientes:
  - OpenStack
  - Keystone
  - Neutron
  - Swift

  Para instalar los clientes de línea de mandatos de OpenStack, consulte Instalar los clientes de línea de mandatos de OpenStack.
- Biblioteca Paramiko para acceso remoto en Python.

  Nota: Si desea instalar Agente de OpenStack en un servidor RedHat Linux nuevo, antes de instalar la biblioteca Paramiko, ejecute el mandato siguiente para instalar el software necesario:

  ```
  wget https://ftp.dlitz.net/pub/dlitz/crypto/pycrypto/pycrypto-2.6.1.tar.gz
  yum install gcc/openssl-devel/libffi-devel
  ```
- KornShell

Agente de Oracle Database

En Red Hat Enterprise Linux versión 5 y versión 6 y SUSE Linux Enterprise Server versión 11 y versión 12 x64, si el Agente de Oracle Database supervisa la base de datos Oracle de forma remota, debe

instalar primero los clientes instantáneos de Oracle. Instale los clientes instantáneos de Oracle desde Oracle Technology Network - Instant Client Downloads.

el cliente instantáneo v10.x, v11.x y v12.x están soportados en el Agente de Oracle Database.

Agente de PHP

Si la aplicación PHP se despliega mediante el usuario root, debe utilizar el usuario root para instalar, configurar, iniciar o detener el agente. Si la aplicación PHP se despliega mediante un usuario no root, puede utilizar el usuario root o el mismo usuario no root para instalar, configurar, iniciar o detener el agente.

Debe tener instalada una aplicación WordPress existente. El Agente de PHP supervisa WordPress V3.7.1 o posterior.

El agente solo evalúa el rendimiento de las peticiones PHP en aplicaciones WordPress. No se evalúan las cargas de CSS y JS.

El agente no utiliza argumentos de URL para identificar los URL.

Recopilador de datos de Python

El Recopilador de datos de Python supervisa aplicaciones Django.

Agente de Supervisión de tiempo de respuesta

Antes de instalar el Agente de Supervisión de tiempo de respuesta, revise la sección de planificación de la instalación aquí: “Planificación de la instalación ” en la página 712.

Agente de SAP HANA Database

1. Instale el cliente HDBSQL del cliente de base de datos SAP HANA versión 1.00.102.06 o posterior en el sistema Linux.

   Importante: Para el sistema operativo RHEL 5.x de 64 bits, instale Linux SUSE 9 en el cliente de base de datos SAP HANA x86_64 64bit en lugar de Linux en x86_64 64bit. Para los sistemas operativos RHEL 6.x, o posterior de 64 bits, instale Linux en el cliente de base de datos SAP HANA x86_64 64bit.

2. Ejecute el mandato siguiente para añadir la vía de acceso del directorio de instalación a la variable de entorno **LD_LIBRARY_PATH**:

   `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:`*`vía_acceso_directorio_instalación`*

   Ejemplo: `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/sap/hdbclient`, donde `/usr/sap/hdbclient` es la vía de instalación del cliente de base de datos SAP HANA.

Importante:

Si la vía de instalación del cliente de base de datos SAP HANA no se añade a la variable de entorno **LD_LIBRARY_PATH**, el explorador de requisitos previos devuelve el resultado `FAIL`.

La variable de entorno que ha añadido mediante el mandato de exportación, sólo se conserva para la sesión concreta del terminal. Por lo tanto, asegúrese de que ejecuta el script de instalación del agente en el mismo terminal que ha utilizado para añadir la variable de entorno.

Agente de Synthetic Playback

Para instalar el Agente de Synthetic Playback, el usuario de sistema operativo requiere los siguientes permisos:

- Habilite el permiso de lectura y ejecución para la imagen de instalación
- Habilite el permiso de escritura para el inicio del agente

Para ejecutar el Agente de Synthetic Playback, el usuario de sistema operativo requiere los siguientes permisos:

- Habilite el permiso de lectura, escritura y ejecución para la ubicación de instalación del agente y sus subdirectorios y archivos.
- Habilite el permiso para ejecutar Mozilla Firefox.

- Asegúrese de que el binario de ejecución de Mozilla Firefox está en la variable de entorno PATH del perfil del usuario.

Antes de instalar el Agente de Synthetic Playback, debe completar los pasos siguientes:

1. Sincronice ubicaciones de instalación del agente con Consola de Cloud APM.
2. Instale Mozilla Firefox y el servidor de visualización Xvfb.
3. Verifique que el servidor de visualización Xvfb está en funcionamiento. Ejecute el mandato:

   ```
   # Xvfb -ac
   ```

   No debe haber ninguna salida de error.
4. Compruebe que el proceso Xvfb se está ejecutando. Ejecute el mandato siguiente:

   ```
   # ps -ef|grep Xvfb
   ```

   Salida de ejemplo:

   ```
   root 7192 1 0 Jan14 ? 00:00:14 Xvfb -ac
   root 20393 17900 0 02:05 pts/0 00:00:00 grep -i xvfb
   ```
5. Detenga el proceso Xvfb. Ejecute el mandato siguiente:

   ```
   # kill -9 7192
   ```
6. Vaya a *dir_instalación*/etc/hosts y edite el principio del archivo hosts para incluir los parámetros siguientes:

   ```
   127.0.0.1 localhost
   ```

   A continuación, guarde y cierre el archivo hosts.

Agente de WebSphere Applications

Antes de que se instale el agente, el comprobador de requisitos comprueba que *ulimit* está establecido en **524000** en el sistema Linux. Debe ejecutar el mandato **ulimit -d 524000** para asegurarse de que la variable de entorno del sistema *max data segment size* está establecida en **524000**.

Instalación de agentes

Puede instalar cualquier combinación de agentes de supervisión en un sistema gestionado. Por ejemplo, si instala el Agente de Ruby para supervisar las aplicaciones de Ruby On Rails, quizá prefiera instalar también el Agente de Supervisión de tiempo de respuesta, el Agente de sistema operativo Linux o los dos agentes. Con el Agente de Supervisión de tiempo de respuesta, puede recopilar más información de tiempo de respuesta de las aplicaciones de Ruby. Con el Agente de sistema operativo Linux, puede supervisar otros aspectos del sistema, como la CPU global, la memoria y el disco.

La oferta determina qué agentes de supervisión están disponibles para la instalación. Si desea una lista de los agentes incluidos en cada oferta, consulte “Capacidades” en la página 54.

Para obtener una lista de los agentes que se ejecutan en los sistemas Linux, consulte “Instalación de agentes en sistemas Linux” en la página 132.

Antes de empezar

Descargue los agentes. Consulte “Descarga de los agentes y recopiladores de datos” en la página 107.

Revise la información de “Requisitos del sistema” en la página 87 para asegurarse de que cumple los requisitos para los agentes que planea instalar.

Revise las tareas previas a la instalación antes de instalar los agentes. Para obtener detalles, consulte “Preinstalación en sistemas Linux” en la página 134.

Nota: Java Runtime solo se instala cuando el agente lo necesita y no siempre está disponible. Además, ksh ya no es necesario para la instalación del agente, excepto para la instalación del Agente de resumen y poda, que se instala durante la instalación del Servidor de Cloud APM. Se da soporte a SELinux en modalidad de imposición.

Acerca de esta tarea

Puede instalar los agentes de supervisión como un usuario root o no root. Si no tiene privilegios de usuario root y desea instalar un agente de supervisión, puede instalar el agente como usuario no root, consulte "Instalación de agentes como usuarios no root" en la página 146. Además, puede instalar el agente como usuario no root si es administrador del sistema principal y no desea ejecutar el agente de supervisión como usuario root. El flujo de instalación es el mismo que para un usuario root.

Se da soporte a la coexistencia de agentes. Puede instalar agentes de IBM Cloud Application Performance Management en el mismo sistema donde están instalados los agentes de IBM Tivoli Monitoring. Sin embargo, ambos tipos de agente no se pueden instalar en el mismo directorio. Para obtener más información sobre la coexistencia de agentes, consulte "Coexistencia del agente de Cloud APM y el agente de Tivoli Monitoring" en la página 984.

Procedimiento

1. Abra una sesión shell de terminal en el sistema Red Hat Enterprise Linux.
2. En el sistema, navegue al directorio donde ha descargado el archivo tar

   Los agentes deben estar instalados en el sistema donde esté instalada la aplicación que desea supervisar. Si es necesario, transfiera el archivo de archivado de instalación al sistema para que se pueda supervisar. El archivo de archivado contiene el script de instalación y el de agente.

   Recuerde: Asegúrese de que el directorio no contiene una versión más antigua del archivo de archivado.
3. Extraiga los archivos de instalación de mediante los mandatos siguientes, que dependen de la oferta:

   ```
   tar -xf ./archivos_instalación.tar
   ```

   donde *archivos_instalación* es el nombre del archivo de instalación correspondiente a su oferta.

   El script de instalación se extrae en un directorio especificado para el archivo de archivado y la versión. Por ejemplo: *oferta*_Agent_Install_8.1.4.0. El archivo binario del agente y los archivos relacionados con la configuración se extraen en los subdirectorios dentro de este directorio.
4. Ejecute el script de instalación desde el directorio que se llama para el archivo de archivado y la versión:

   ```
   ./installAPMAgents.sh
   ```

   Para instalar los agentes en modalidad silenciosa, consulte "Instalación silenciosa de agentes" en la página 149.
5. Especifique si desea instalar agentes individuales, una combinación de los agentes o todos los agentes.
6. En función de si está instalando o actualizando los agentes, realice uno de los pasos siguientes:
   - Si está instalando los agentes, especifique el directorio de inicio de instalación del agente o utilice el directorio predeterminado aplicable:
     - `/opt/ibm/apm/agent`
   - Si está actualizando los agentes, después de que se le solicite el directorio de inicio de instalación de los agentes, especifique el directorio de instalación de la versión anterior de los agentes.
     a. Si existe una versión más antigua de los agentes en el directorio `/opt/ibm/apm/agent`, debe especificar un directorio de instalación nuevo. En el paso siguiente, se le preguntará si desea migrar la configuración del agente desde el directorio `/opt/ibm/apm/agent`.

b. Si confirma que desea migrar la configuración de agente del directorio de instalación antiguo (`/opt/ibm/ccm/agent`) al directorio de instalación nuevo, por ejemplo `/opt/ibm/apm/agent`, debe iniciar el agente en la ubicación de instalación nueva.

   Restricción: La versión más antigua del agente se detiene automáticamente en la ubicación de instalación antigua, pero no se inicia automáticamente en la ubicación de instalación nueva.

c. Tras verificar que la instalación se ha completado y que el agente funciona en el nuevo directorio de instalación, debe desinstalar la versión más antigua del agente desde el directorio `/opt/ibm/ccm/agent`. Si desea eliminar todos los agentes, ejecute el mandato **`/opt/ibm/ccm/agent/bin/smai-agent.sh uninstall_all`**.

7. Cuando se le pregunte si acepta el acuerdo de licencia, entre 1 para aceptar el acuerdo y continuar, o entre 2 para rechazarlo.

   Tras entrar 1 (aceptar), se inicia una exploración de requisitos previos del entorno y tarda unos pocos minutos en completarse. Si faltan algunos requisitos, un mensaje le dirigirá a un archivo de registro que contiene la causa del error. La falta de un requisito previo, como por ejemplo la falta de una biblioteca o espacio de disco insuficiente detendrá la instalación. Debe resolver la anomalía y volver a iniciar el script de instalación.

   Nota: Si la instalación existe con el mensaje siguiente, compruebe si se ha iniciado el servicio del servidor (Inicio -> Herramientas administrativas -> Servicios). Si no es así, inicie el servicio del servidor y vuelva a ejecutar `installAPMAgents.bat`.

   ```
   Este script [installAPMAgents.bat] se debe ejecutar como Administrador.
   ```

8. Si ha instalado los agentes mediante un ID de usuario no root, debe actualizar los scripts de arranque del sistema (consulte “Instalación de agentes como usuarios no root” en la página 146).
9. Cuando se haya completado la instalación y la línea de mandatos esté disponible, puede repetir los pasos de este procedimiento para instalar más agentes de supervisión en el sistema gestionado.

Qué hacer a continuación

Configure el agente como sea necesario. Si el agente de supervisión requiere configuración como se describe en Capítulo 5, “Despliegue de agentes y recopiladores de datos”, en la página 117 o si desea revisar los valores predeterminados, consulte Capítulo 7, “Configuración del entorno”, en la página 165.

- Si utiliza un proxy directo porque el cortafuegos no permite conexiones HTTPS salientes transparentes a hosts externos, debe editar el archivo de configuración de entorno del agente. Para obtener instrucciones, consulte “Configuración de agentes para la comunicación mediante un proxy directo” en la página 165.
- Si ha actualizado un agente desde una versión anterior, identifique cualquier tarea de reconfiguración o migración que debe completar antes de iniciar sesión en la Consola de Cloud APM. Para obtener información sobre esas tareas, consulte “Actualización de los agentes” en la página 1173. Después de una actualización, debe reiniciar todos los agentes que el instalador no configura e inicia automáticamente.

Para iniciar un agente, ejecute el mandato siguiente:

```
./nombre-agent.sh start
```

Para obtener más información sobre los mandatos de agente de supervisión, incluido el nombre que se va a utilizar, consulte “Utilización de mandatos de agente” en la página 184. Si desea información sobre qué agentes se inician de forma automática y manual, consulte Capítulo 5, “Despliegue de agentes y recopiladores de datos”, en la página 117.

Después de una actualización, debe reiniciar todos los agentes que el instalador no configura e inicia automáticamente.

Después de configurar e iniciar el agente, vea los datos que el agente está recopilando.

- Si no ha iniciado sesión, siga las instrucciones en “Inicio de la Consola de Cloud APM” en la página 1009.

- Si desea ver sistemas gestionados del dominio de IBM Tivoli Monitoring en los Panel de instrumentos del rendimiento de aplicaciones, complete las tareas descritas en “Integración con IBM Tivoli Monitoring V6.3 ” en la página 983.

Instalación de agentes en sistemas Windows

Puede instalar algunos de los agentes de supervisión Cloud APM en sistemas Windows.

Los agentes de supervisión siguientes están soportados en sistemas Windows de 64 bits. Donde se indique, los agentes también están soportados en sistemas Windows de 32 bits.

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HTTP Server*
- Monitoring Agent for IBM Cloud
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Internet Services*
- Monitoring Agent for MQ Appliance
- Monitoring Agent for JBoss
- Monitoring Agent for MariaDB
- Monitoring Agent for Microsoft Active Directory*
- Monitoring Agent for Microsoft Cluster Server*
- Monitoring Agent for Microsoft Exchange Server
- Monitoring Agent for Microsoft Hyper-V Server
- Monitoring Agent for Microsoft Internet Information Services
- Monitoring Agent for Skype for Business Server (anteriormente conocido como Microsoft Lync Server)*
- Monitoring Agent for Microsoft .NET
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent for Microsoft SharePoint Server
- Monitoring Agent for Microsoft SQL Server*
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for Oracle Database
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sterling Connect Direct

- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for Sybase Server
- Monitoring Agent for Tomcat
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ
- Monitoring Agent for Windows OS*
- Agente de Supervisión de tiempo de respuesta*

* Está soportado en ambos sistemas Windows, de 32 y 64 bits.

Preinstalación en sistemas Windows

Debe llevar a cabo las tareas de preinstalación necesarias antes de instalar los agentes en los sistemas Windows. Algunas tareas de preinstalación son específicas del agente y otras tareas se aplican a varios agentes.

Nota: Estos requisitos son adicionales a los requisitos identificados en los Informes de compatibilidad de productos de software.

Para conocer los requisitos de versión actuales y las dependencias del agente, consulte System requirements (APM Developer Center) para obtener un enlace a los informes de compatibilidad de productos de software.

Todos los agentes

Las tarea de preinstalación siguientes son aplicables a todos los agentes:

Probar la conectividad
Antes de instalar los agentes, asegúrese de que el sistema puede comunicarse con el Servidor de Cloud APM. Para obtener información sobre la comprobación de conectividad con el Servidor de Cloud APM, consulte Conectividad de red.

Instalación desde el indicador de mandatos en una unidad local
Utilice el indicador de mandatos de Windows para iniciar el script de instalación. No utilice Windows PowerShell para iniciar el script de instalación.

Copie los archivos de instalación en un disco local o en una unidad de red correlacionada y, a continuación, inicie el script de instalación. No inicie el script de instalación desde una ubicación de red.

Inicie el script de instalación desde un nuevo indicador de mandatos. No inicie el script de instalación desde un indicador de mandatos existente debido a que el indicador de mandatos podría tener variables de entorno obsoletas.

Establecimiento de la variable de entorno *CANDLEHOME*
Si previamente utilizó ITM Agent Converter para instalar y configurar un agente en el mismo sistema gestionado, la variable de entorno *CANDLEHOME* ha cambiado a ese directorio en el que instaló el agente con Agent Converter. Antes de instalar y configurar un agente Cloud APM nativo, debe establecer la variable de entorno *CANDLEHOME* en un directorio diferente, de lo contrario, el agente Cloud APM no se puede iniciar.

Agentes específicos

Las tareas de preinstalación siguientes son aplicables a los agentes especificados:

Agente de DataStage

1. Habilite los parámetros en el archivo `DSODBConfig.cfg`. Complete los pasos siguientes:
   a. Abra el archivo `DSODBConfig.cfg` en la ubicación siguiente de un editor:

dir_instalación_servidor_información_infosphere\Server\DSODB

b. Descomente los parámetros siguientes eliminado el símbolo *#*:

MonitorLinks=1
JobRunUsage=1
ResourceMonitor=1
DSODBON=1

c. Edite los valores de estos parámetros igual que 1.

2. Copie el controlador JDBC de la base de datos que se utiliza para la configuración del repositorio de metadatos en el sistema agente.

a. JDBC 4 tipo 4 o posterior. Ejemplo: `db2jcc4.jar`

b. Controlador JDBC tipo 4 para Oracle. Ejemplo: `ojdbc6.jar`

c. Controlador JDBC para MS SQL:

- `Sqljdbc41.jar` requiere un JRE de 7 y da soporte a la API de JDBC 4.1.
- `Sqljdbc42.jar` requiere un JRE de 8 y da soporte a la API de JDBC 4.2.

Agente de IBM Integration Bus

Asegúrese de que el ID de usuario para instalar el Agente de IBM Integration Bus se encuentra en el grupo de usuarios `mqbrkrs`.

Internet Service Monitoring

Para Internet Service Monitoring, debe aplicar el arreglo temporal 3 de la infraestructura principal de IBM Cloud Application Performance Management 8.1.4.0 en el servidor APM desde aquí y a continuación preconfigurar el agente. El agente y el módulo de puente utilizan los puertos 9510 y 9520. En caso de que estos puertos ya estén en uso, la instalación no continuará.

Nota:

- Para los usuarios existentes se recomienda instalar el agente de Internet Service Monitoring en plataformas de 64 bits ya sea Windows o Linux en lugar de actualizar el agente de una plataforma Windows de 32 bits a una nueva versión.
- El agente de Internet Service Monitoring no da soporte a Windows 2008 R2 en la plataforma Windows de 64 bits.

Agente de MySQL

Para Monitoring Agent for MySQL, debe instalar el servidor MySQL y el controlador JDBC MySQL antes de instalar Agente de MySQL en ese sistema. Para instalar el controlador JDBC, consulte Controlador JDBC de MySQL Connector/J.

Agente de Oracle Database

Si el Agente de Oracle Database supervisa la base de datos Oracle de forma remota, debe instalar primero los clientes instantáneos de Oracle desde Oracle Technology Network - Instant Client Downloads en los sistemas siguientes:

- Windows Server 2012 64 bits
- Windows Server 2012 R2 64 bits
- Windows Server 2008 R2 Datacenter 64 bits
- Windows Server 2008 R2 Enterprise 64 bits
- Windows Server 2008 R2 Standard 64 bits

Los clientes instantáneos v10.x, v11.x y v12.x están soportados en el Agente de Oracle Database.

Agente de Supervisión de tiempo de respuesta

Antes de instalar el Agente de Supervisión de tiempo de respuesta, revise la sección de planificación de la instalación aquí: “Planificación de la instalación ” en la página 712.

Agente de SAP HANA Database

1. Instale el cliente HDBSQL del cliente de base de datos SAP HANA versión 1.00.102.06 o posterior en el sistema Windows.
2. Añada la vía de acceso de instalación del cliente SAP HANA a la variable de entorno **PATH**.

   Ejemplo: Añada `C:\Program Files\sap\ehdbclient` a la variable de entorno **PATH**, donde `C:\Program Files\sap\hdbclient` indica la vía de acceso de instalación del cliente de base de datos de SAP HANA.

Agente de Tomcat

1. El SDK Java está instalado en el servidor Tomcat donde está instalado el agente.
2. La vía de acceso del SDK se añade a la variable *PATH* directamente o mediante el mandato **set path** antes de instalar el agente.
3. El mandato **JAR** está en funcionamiento.

Instalación de agentes

Puede instalar cualquier combinación de agentes de supervisión en un sistema gestionado. Por ejemplo, si instala el Monitoring Agent for MySQL para supervisar los servidores MySQL, quizá prefiera instalar también el Agente de Supervisión de tiempo de respuesta para recopilar información de tiempo de respuesta adicional para sus aplicaciones de Ruby. Quizá prefiera instalar también el Monitoring Agent for Windows OS para supervisar otros aspectos del sistema, como la CPU global, la memoria y el disco.

La oferta determina qué agentes de supervisión están disponibles para la instalación. Si desea una lista de los agentes incluidos en cada oferta, consulte "Capacidades" en la página 54.

Para obtener una lista de los agentes que se ejecutan en un sistema Windows, consulte "Preinstalación en sistemas Windows" en la página 142.

Antes de empezar

Descargue los agentes. Consulte "Descarga de los agentes y recopiladores de datos" en la página 107.

Revise la información de "Requisitos del sistema" en la página 87 para asegurarse de que cumple los requisitos para los agentes que planea instalar.

Revise las tareas de requisito previo de agentes antes de instalar los agentes. Para obtener detalles, consulte "Preinstalación en sistemas Windows" en la página 142.

Acerca de esta tarea

Asegúrese de que tiene el permiso adecuado para ejecutar el script de instalación de agente y los mandatos de agente. Debe haber iniciado la sesión utilizando uno de los siguientes tipos de cuenta de usuario:

- cuenta de usuario administrador de Windows predeterminado
- cuenta de usuario administrador
- cuenta de usuario que sea miembro del grupo de administradores
- cuenta de usuario que esté registrada como administrador en los servicios de Active Directory

Se da soporte a la coexistencia de agentes. Puede instalar agentes de IBM Cloud Application Performance Management en el mismo sistema donde están instalados los agentes de IBM Tivoli Monitoring. Sin embargo, ambos tipos de agente no se pueden instalar en el mismo directorio. Para obtener más información sobre la coexistencia de agentes, consulte "Coexistencia del agente de Cloud APM y el agente de Tivoli Monitoring" en la página 984.

Procedimiento

Siga estos pasos para instalar los agentes de supervisión en máquinas virtuales y sistemas en los que esté instalado el sistema operativo Windows:

1. En el sistema, vaya al directorio donde ha descargado el archivo comprimido.
2. Extraiga los archivos de instalación del agente para la oferta (u ofertas) en la ubicación donde desea instalar el software del agente de supervisión.
   El script de instalación .bat se extrae en un directorio especificado para el archivo de archivado y la versión. Por ejemplo: *oferta*_Agent_Install_8.1.4.0. El archivo binario del agente y los archivos relacionados con la configuración se extraen en los subdirectorios dentro de este directorio.
3. Abra un indicador de mandatos como administrador.
   a) En el menú **Inicio**, escriba comando en el cuadro de búsqueda.
   b) Pulse el botón derecho (del ratón) en el **Símbolo del sistema** en la lista que se muestra y seleccione **Ejecutar como administrador**.
4. En el indicador de mandatos, ejecute el script de instalación con privilegios de administrador desde el directorio especificado para el archivo de archivado y versión:

   ```
   cd oferta_Agent_Install_versión
   installAPMAgents.bat
   ```

   Restricción: Para el Agente de WebSphere Applications, los privilegios de administrador debe ser los mismos privilegios que se han utilizado para instalar WebSphere Application Server.

   Para instalar los agentes en modalidad silenciosa, consulte "Instalación silenciosa de agentes" en la página 149.
5. Si está instalando los agentes, proporcione el nombre del directorio de instalación.

   La vía de acceso de instalación predeterminada es C:\IBM\APM. El nombre del directorio de instalación no puede superar los 80 caracteres ni contener caracteres no ASCII, caracteres especiales o de doble byte. Los nombres de directorio de la vía de acceso solo pueden contener los caracteres siguientes: abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ _ \:0123456789()~-./.

   Nota: Si la creación de nombres de archivo cortos (*8dot3Name*) está inhabilitada, si los nombres de directorio de la vía de acceso contienen espacios, la instalación no está soportada.

   Si está actualizando el agente, este paso no es necesario y el agente se instala en el directorio de instalación anterior.
6. Cuando se le pregunte si acepta el acuerdo de licencia, entre 1 para aceptar el acuerdo y continuar, o entre 2 para rechazarlo.

   Tras entrar 1 (aceptar), se inicia una exploración de requisitos previos del entorno y tarda unos pocos minutos en completarse. Si faltan algunos requisitos, un mensaje le dirigirá a un archivo de registro que contiene la causa del error. La falta de un requisito previo, como por ejemplo la falta de una biblioteca o espacio de disco insuficiente detendrá la instalación. Debe resolver la anomalía y volver a iniciar el script de instalación.

   Nota: Si la instalación existe con el mensaje siguiente, compruebe si se ha iniciado el servicio del servidor (Inicio -> Herramientas administrativas -> Servicios). Si no es así, inicie el servicio del servidor y vuelva a ejecutar installAPMAgents.bat.

   ```
   Este script [installAPMAgents.bat] se debe ejecutar como Administrador.
   ```
7. Una vez completada la instalación y disponible el indicador de mandatos, repita estos pasos para instalar más agentes de supervisión.

Qué hacer a continuación

Configure los agentes según sea necesario. Para comprobar si el agente de supervisión requiere configuración manual, consulte Capítulo 5, "Despliegue de agentes y recopiladores de datos", en la página 117. Para obtener instrucciones de configuración, o si desea revisar los valores de configuración predeterminados, consulte Capítulo 7, "Configuración del entorno", en la página 165.

Antes de instalar nuevos agentes, Windows Installer detiene temporalmente todos los agentes actualmente en ejecución en la ubicación del producto instalado. Una vez finalizada la instalación, el

instalador reinicia todos los agentes detenidos. Debe reiniciar manualmente los agentes de supervisión que no se hayan configurado automáticamente mediante el instalador.

- Si utiliza un proxy directo porque el cortafuegos no permite conexiones HTTPS salientes transparentes a hosts externos, debe editar el archivo de configuración de entorno del agente. Para obtener instrucciones, consulte "Configuración de agentes para la comunicación mediante un proxy directo" en la página 165.
- Si ha actualizado un agente desde una versión anterior, identifique cualquier tarea de reconfiguración o migración que debe completar antes de iniciar sesión en la Consola de Cloud APM. Para obtener información sobre esas tareas, consulte "Actualización de los agentes" en la página 1173.

Utilice uno de los métodos siguientes para iniciar el agente:

- Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**. Pulse el botón derecho del ratón en un agente y pulse **Iniciar**.
- Ejecute el mandato siguiente

```
nombre-agent.bat start
```

Para obtener más información sobre los mandatos de agente de supervisión, incluido el nombre que se va a utilizar, consulte "Utilización de mandatos de agente" en la página 184. Si desea información sobre qué agentes se inician de forma automática y manual, consulte Capítulo 5, "Despliegue de agentes y recopiladores de datos", en la página 117

Después de una actualización, debe reiniciar todos los agentes que el instalador no configura e inicia automáticamente.

Después de configurar e iniciar el agente, vea los datos que el agente está recopilando.

- Si no ha iniciado sesión, siga las instrucciones en "Inicio de la Consola de Cloud APM" en la página 1009.
- Si desea ver sistemas gestionados del dominio de IBM Tivoli Monitoring en los Panel de instrumentos del rendimiento de aplicaciones, complete las tareas descritas en "Integración con IBM Tivoli Monitoring V6.3 " en la página 983.

Instalación de agentes como usuarios no root

Si no tiene privilegios de usuario root y desea instalar un agente de supervisión, puede instalar el agente como usuario no root. Además, puede instalar el agente como usuario no root si es administrador del sistema principal y no desea ejecutar el agente de supervisión como usuario root. El flujo de instalación es el mismo que para un usuario root. Después de una instalación no root, ejecute el script **UpdateAutoRun.sh** con acceso de usuario rooto sudo.

Antes de empezar

Para identificar de forma exclusiva el sistema, el Agente de sistema operativo Linux debe identificar el Universal Unique Identifier (UUID) de la placa del sistema, el fabricante, el modelo y el número de serie. Esta información es necesaria antes de añadir el agente a una aplicación en la consola de Cloud APM.

Obtenga la información del sistema verificando que existen las entidades siguientes en el sistema:

1. Compruebe que el mandato **/usr/bin/hal-get-property** esté instalado en el sistema y que el proceso hald (daemon HAL) esté en ejecución. Si el mandato no está instalado, continúe en el paso 2. Si el mandato está instalado, omita el paso 2 y el paso 3. Nota: si la versión de sistema operativo es Red Hat 7, el proceso hald no estará disponible.
2. Si el mandato **/usr/bin/hal-get-property** no está instalado en el sistema, confirme que el archivo `/sys/class/dmi/id/product_uuid` existe y que contiene el UUID del sistema, y que el usuario que instala el agente de sistemas operativo Linux tiene acceso de lectura a este archivo. Si este archivo no existe, continúe en el paso 3. Si el archivo existe, omita el paso 3.
3. Si el mandato **/usr/bin/hal-get-property** no está instalado y el archivo `/sys/class/dmi/id/product_uuid` no existe, debe asegurarse de que los mandatos **hostname** o **hostnamectl**

devuelven el nombre de host completo. Si estos mandatos devuelven el nombre de host abreviado sin el dominio, debe establecer el nombre de host completo especificando los mandatos **"hostname <fqhn>"** o **"hostnamectl set-hostname <fqhn>"**, donde *<fqhn>* debe sustituirse por el nombre de host completo.

Nota: El Agente de sistema operativo Linux recupera esta información periódicamente, por lo que los mandatos o archivos de los pasos anteriores deben permanecer implementados incluso después de la instalación.

Nota: El agente del sistema operativo Linux no da soporte a la supervisión de Docker cuando se ejecuta como usuario no root.

Procedimiento

1. Instale los agentes de supervisión en Linux o UNIX tal como se describe en "Instalación de agentes en sistemas Linux" en la página 132 y "Instalación de agentes en sistemas UNIX" en la página 126.
2. Opcional: Si ha instalado el agente como un usuario seleccionado y desea configurar el agente como un usuario distinto, ejecute el script `./secure.sh`.

   Para obtener más información sobre el script **./secure.sh**, consulte "Configuración de agentes como usuarios no root" en la página 191 y Asegurar los archivos de instalación de agente.

   Por ejemplo: **./secure.sh -g db2iadm1**
3. Opcional: Configure los agentes de supervisión en Linux o UNIX según sea necesario; consulte Capítulo 7, "Configuración del entorno", en la página 165.
4. Para actualizar los scripts de arranque del sistema, ejecute el script siguiente con acceso de usuario rooto sudo: *dir_instalación*`/bin/UpdateAutoRun.sh`

Qué hacer a continuación

Si ha instalado el agente mediante un usuario no root y desea configurar el agente mediante el mismo usuario, no se necesita ninguna acción especial. Si ha instalado el agente mediante un usuario seleccionado y desea configurar el agente mediante un usuario distinto, consulte "Configuración de agentes como usuarios no root" en la página 191.

Si ha instalado y configurado el agente mediante un usuario no root y desea iniciar el agente mediante el mismo usuario, no se necesita ninguna acción especial. Si ha instalado y configurado el agente mediante un usuario seleccionado y desea iniciar el agente mediante un usuario distinto, consulte "Inicio de agentes mediante un usuario no root" en la página 1047.

Utilice el mismo ID de usuario para la instalación del agente y para las actualizaciones.

Si ejecuta el script **UpdateAutoRun.sh** como usuario root, el agente se configura para iniciarse automáticamente después de reiniciar el sistema operativo. Si no desea que el agente se comporte así, puede inhabilitar el inicio automático de agente. Para obtener más información, consulte "Inhabilitación del inicio automático de agente en sistemas UNIX y Linux" en la página 191.

Asegurar los archivos de instalación de agente

Después de instalar los agentes de supervisión como usuario no root en sistemas Linux o UNIX, puede ejecutar el script `secure.sh` para asegurar la instalación del agente eliminando permisos de grabación y estableciendo la propiedad de archivos correcta.

Antes de empezar

- Debe tener permisos de lectura, grabación y ejecución sobre el directorio de instalación.
- La instalación de los agentes de supervisión y cualquier configuración de agente debe haberse completado en el sistema y los agentes deben haberse iniciado satisfactoriamente.
- Si está ejecutando agentes como cuentas de usuario diferentes, deben ser miembros del mismo grupo. (Consulte la opción `-g`.)

Acerca de esta tarea
Siga este paso para bloquear los permisos de archivo en la instalación. Hay opciones disponibles para solicitar una contraseña no root, para especificar un nombre de grupo y para ver ayuda para el mandato.

Procedimiento

- Ejecute el mandato siguiente desde el directorio *dir_instalación*/bin. Uso:

```
secure.sh [-g grupo_común] [-n] [-h]
```

  - En la modalidad más simple, ejecute el script **./secure.sh**, que elimina los permisos de grabación y establece el usuario actual y el grupo de usuarios como propietarios de archivo. Si el script es ejecutado por un usuario no root, se solicita al usuario la contraseña raíz.
  - Si un usuario no root ejecuta el script **./secure.sh** con la opción -n, no se solicita a este usuario una contraseña raíz. En este caso, el cambio de los permisos de archivo y el cambio de propiedad se realizan utilizando los privilegios de este usuario. Si el directorio de instalación contiene archivos que son propiedad de diferentes usuarios y el usuario actual no tiene privilegios para modificar los permisos y la propiedad de los archivos de otro usuario, esta modalidad puede fallar.
  - Si desea establecer un grupo determinado como propietario del grupo, el propietario debe proporcionar la opción -g con un nombre de grupo válido como argumento a dicha opción. (Consulte Ejemplo.)
    Ejecute secure.sh -g *grupo_común*.
    El mandato cambia la propiedad de los archivos y los directorios de forma recursiva.

    Si el *grupo_común* no es el grupo primario del usuario, puede establecer el *grupo_común* como grupo propietario de los archivos nuevos creados en un directorio, ejecutando el mandato siguiente:

    ```
    chmod g+s dir_instalación/bin/sub_dir
    ```

    donde *sub_dir* es cualquier subdirectorio, por ejemplo /opt/ibm/ccm/agent.
  - Ejecute el script **./secure.sh** con la opción –h para obtener información de ayuda para el script.

Resultados
El directorio de instalación permite el acceso al usuario que ejecutó el script o solo a los usuarios del grupo especificado.

Ejemplo

Si el usuario Alice es un miembro del grupo del sistema llamado "apmgroup", puede utilizar el grupo para establecer la propiedad del grupo con el mandato siguiente:

```
./secure.sh -g apmgroup
```

Después de ejecutar el script, el grupo se establece como "apmgroup" para todos los archivos en el *dir_instalación* para el grupo.

Qué hacer a continuación

La ejecución del script **./secure.sh** debe resultar en el establecimiento de los siguientes permisos para los agentes.

```
rwx rwx ---
```

Tras ejecutar el script, compruebe los permisos para los archivos de agente. Por ejemplo, para Supervisión de tiempo de respuesta, compruebe los archivos en *dir_instalación*/*arch*/hu/lib/mod_wrt.so. Si los permisos para estos archivos no están definidos correctamente, actualice los permisos manualmente. Por ejemplo, para el Agente de supervisión del tiempo de respuesta:

1. Establezca los permisos, ejecute:

```
chmod g+rx $AGENT_HOME/bin/rt-agent.sh
```

2. Establezca el usuario y el grupo, ejecute:

```
chown
nuevo_usuario:nuevo_grupo
$AGENT_HOME/bin/rt-agent.sh
```

Instalación silenciosa de agentes

La instalación silenciosa de agentes reduce el tiempo de instalación. Para instalar un agente de supervisión en la modalidad silenciosa, debe descargar un archivo de archivado de imagen de instalación de agente desde el sitio de descargas de sitio web de IBM Marketplace, extraer los archivos de instalación de agente, preparar un archivo de respuestas silenciosas y ejecutar el script de instalación en la modalidad silenciosa.

Antes de empezar

1. Revise las tareas de requisito previo necesarias para instalar los agentes de supervisión y descargue y extraiga los archivos de instalación de agente. Para obtener detalles, consulte Instalación de agentes en sistemas UNIX, Instalación de agentes en sistemas Linux o Instalación de agentes en sistemas Windows.
2. Complete los pasos siguientes para preparar un archivo de respuestas silencioso para instalar agentes:
   a. Localice el archivo de instalación silenciosa para su oferta (u ofertas) *oferta*_silent_install.txt, haga una copia de este archivo y ábralo en un editor de texto.
   b. Elimine el comentario del acuerdo de licencia.
   c. Complete uno de los pasos siguientes para especificar los agentes que desea instalar:
      - Elimine el comentario de los agentes específicos a instalar. Por ejemplo:

```
INSTALL_AGENT=os
```

```
INSTALL_AGENT=ruby
```

      - Elimine el comentario de INSTALL_AGENT=all para instalar todos los agentes.
   d. Elimine el comentario de AGENT_HOME y especifique el directorio donde desea instalar los agentes.

      Recuerde: Linux Si está actualizando agentes en un sistema Linux, no debe especificar el directorio /opt/ibm/apm/agent.
   e. Linux Si está actualizando los agentes en un sistema Linux, elimine el comentario de MIGRATE_CONF=yes.
   f. Guarde el archivo.

Procedimiento

1. En la línea de mandatos, vaya al directorio donde ha extraído el script de instalación y ejecute el mandato siguiente:

```
cd oferta_Agent_Install_versión
```

2. Opcional: Este paso SÓLO es necesario para Solaris 10. Debe crear un enlace dinámico a ksh antes de ejecutar el script de instalación en Solaris 10.
   a) Realice una copia de seguridad del mandato /bin/sh:

```
mv /bin/sh /bin/sh.bkup_origin
```

b) Cree un enlace dinámico al mandato ksh:

```
ln -s /bin/ksh /bin/sh
```

c) Confirme que el resultado apunta a ksh:

```
ls -l /bin/sh
```

3. Ejecute el mandato de instalación:

- Linux AIX

```
./installAPMAgents.sh -p vía_acceso_archivo_respuestas_silencioso
```

- Windows

```
installAPMAgents.bat -p vía_acceso_archivo_respuestas_silencioso
```

La instalación de los agentes fallará en Windows si el escáner de requisitos previos no puede obtener el tipo de disco en el que se instalará el agente. Si esto se produce, verá un resultado de error para la propiedad validDestLocation en el archivo de registro de instalación. En este caso, puede saltarse la exploración de requisitos previos añadiendo SKIP_PRECHECK= 1 al mandato de instalación. Por ejemplo:

```
installAPMAgents.bat -p vía_acceso_archivo_respuestas_silencioso SKIP_PRECHECK=1
```

Nota: Windows Si la creación de nombres de archivo cortos (*8dot3Name*) está inhabilitada, si los nombres de directorio de la vía de acceso contienen espacios, la instalación no está soportada.

Resultados
Se instalan los agentes.

Qué hacer a continuación

Configure los agentes. Consulte el procedimiento y la tabla de mandatos para sistemas Linux y UNIX y para sistemas Windows.

Eludir la exploración de requisitos previos

Cuando instala los agentes de supervisión, se inicia una exploración de requisitos previos del entorno que tarda unos minutos en completarse. Si faltan algunos requisitos, un mensaje le dirigirá a un archivo de registro que contiene la causa del error. En algunos escenarios de instalación, es posible que desee ignorar los mensajes de aviso o eludir por completo la comprobación de requisitos previos.

Acerca de esta tarea

Hay dos niveles de mensajes de error, WARN y FAIL, y hay dos niveles de elusión:

- El establecimiento de la variable **IGNORE_PRECHECK_WARNING** hace que el instalador ignore los mensajes de aviso (WARN).
- El establecimiento de la variable **SKIP_PRECHECK** hace que el instalador ignore todos los mensajes de error.

Si la instalación de agente ha fallado y ha recibido un aviso (WARN) del comprobador de requisitos previos, revise el aviso. Si desea continuar con la instalación, establezca **IGNORE_PRECHECK_WARNING** e instale de nuevo.

En un entorno en el que tiene imágenes de máquinas virtuales que sirven como plantillas, la exploración de requisitos previos que se lleva a cabo antes de iniciar la instalación solo se puede hacer en la primera imagen de plantilla. Si una imagen de máquina virtual pasa la exploración, el resto de máquinas virtuales creadas a partir de esa imagen también pasarán. Puede ahorrar tiempo eludiendo la comprobación de

requisitos para otras máquinas virtuales creadas a partir de la misma imagen. Establezca la variable **SKIP_PRECHECK** e instale de nuevo.

El valor **SKIP_PRECHECK** también es apropiado para el escenario donde tiene un nuevo sistema operativo que el soporte de IBM o los informes de compatibilidad de producto de software indican que se soporta pero el comprobador de requisitos previos aún no se ha actualizado. Asegúrese primero de intentar instalar el agente, comprobar el registro y asegurarse de que este nuevo sistema operativo es el único elemento que falla, y el único elemento que está eludiendo, porque **SKIP_PRECHECK** hace que el instalador eluda cada elemento de la lista de comprobación de requisitos previos.

Después de descargar y extraer los archivos de instalación, siga este procedimiento para ignorar los mensajes de aviso o para eludir la exploración de requisitos previos.

Procedimiento

En el sistema en el que va a instalar agentes de supervisión, especifique uno de los mandatos siguientes:

- Ignorar los mensajes de aviso (WARN) durante la comprobación de requisitos previos:
  - Linux AIX `export IGNORE_PRECHECK_WARNING=1`
  - Windows `set IGNORE_PRECHECK_WARNING=1`
- Eludir la exploración de requisitos previos:
  - Linux AIX `export SKIP_PRECHECK=1`
  - Windows `set SKIP_PRECHECK=1`

Qué hacer a continuación

Para restaurar el valor predeterminado la próxima vez que desee instalar el agente con el escáner de requisitos previos, desactive la variable **IGNORE_PRECHECK_WARNING** o **SKIP_PRECHECK**:

- Linux AIX `unset IGNORE_PRECHECK_WARNING`
- Windows `set IGNORE_PRECHECK_WARNING=`

o

- Linux AIX `unset SKIP_PRECHECK`
- Windows `set SKIP_PRECHECK=`

Desinstalación de los agentes

Desinstale un único agente o todos los agentes de un sistema gestionado.

Antes de empezar

Para agentes de varias instancias, debe eliminar todas las instancias del agente antes de desinstalar el agente. De lo contrario, las entradas del agente no se borran del registro. Para eliminar instancias, ejecute el mandato siguiente:

- Windows *nombre*`-agent.bat remove` *nombre_instancia*
- Linux AIX `./`*nombre*`-agent.sh remove` *nombre_instancia*

Donde *nombre* es el nombre del agente y *nombre_instancia* es el nombre de la instancia. Para obtener más información, consulte “Utilización de mandatos de agente” en la página 184. Para obtener una lista de los agentes de varias instancias, consulte Tabla 7 en la página 119.

Para los siguientes agentes, una tarea específica del agente debe completarse antes de llevar a cabo el procedimiento de desinstalación:

- Para el Monitoring Agent for HTTP Server, debe suprimir la sentencia `Include` del archivo `http.conf`, por ejemplo, `"Include "/opt/ibm/apm/agent/tmp/khu/kvm65s2_8044.conf"`, antes de reiniciar el servidor IBM HTTP.
- Para el Monitoring Agent for Python, ejecute *dir_instalación*`/lx8266/pg/bin/uninstall.sh` para eliminar códigos de inyección antes de desinstalar el agente.
- Para Monitoring Agent for PHP, ejecute *dir_instalación*`/bin/lx8266/pj/lib/uninstall.`*nombre_instancia*`.sh` para mover códigos de inyección antes de desinstalar el agente.
- Para Monitoring Agent for WebSphere Applications, debe desconfigurar el recopilador de datos para las instancias de servidor supervisadas antes de desinstalar el agente. Siga las instrucciones de "Agente de WebSphere Applications: Desconfiguración del recopilador de datos" en la página 154.

  Para el Agente de WebSphere Applications, asegúrese de que el ID de usuario, que se utiliza para desinstalar el agente, tiene permisos de lectura y grabación completos sobre los directorios `logs` y `runtime` y sobre todos los subdirectorios y archivos que contiene dentro del directorio de inicio del recopilador de datos. El directorio de inicio del recopilador de datos es el siguiente:

  – Windows *dir_instalación*`\dchome\7.3.0.14.08`
  – Linux AIX *dir_instalación*`/yndchome/7.3.0.14.08`
- Para el Agente de Node.js, debe eliminar el plug-in de supervisión de la aplicación Node.js antes de desinstalar el agente. Siga las instrucciones de "Agente de Node.js: eliminación del plug-in de supervisión" en la página 162.
- Para el Agente de Microsoft .NET, debe eliminar el recopilador de datos de las aplicaciones .NET antes de desinstalar el agente. Siga las instrucciones de "Agente de Microsoft .NET: eliminación del recopilador de datos .NET" en la página 163.
- Para el Agente de IBM Integration Bus, si ha configurado el rastreo de transacciones para los intermediarios con la salida de usuario proporcionada por el agente, debe eliminar la salida de usuario antes de desinstalar el agente. Siga las instrucciones que encontrará en "Eliminación de la salida de usuario KQIUserExit" en la página 301.
- Para Internet Service Monitoring, vaya a `<inicio_candle>\BIN` y ejecute el archivo ism-agent.bat con `uninstall` como argumento. En caso de que desee desinstalar todos los agentes de supervisión en el servidor mediante smai-agent.bat, ejecute primero ism-agent.bat con `uninstall` como argumento y a continuación ejecute smai-agent.bat
- Para Monitoring Agent for SAP NetWeaver Java Stack, antes de desinstalar el agente, detenga todas las instancias de agente de pila Java de SAP NetWeaver utilizando el mandato siguiente:

  – Windows `sap_netweaver_java_stack-agent.bat stop nombre_instancia`

Acerca de esta tarea

El agente de Oracle en sistemas Windows solo se puede desintalar mediante el indicador de mandatos.

Procedimiento

1. En la máquina virtual o en el sistema donde se ha instalado el agente de supervisión (o los agentes), inicie una línea de mandatos y vaya al directorio binario:
   - Linux AIX *dir_instalación*`/bin`
   - Windows *dir_instalación*`\BIN`

   donde *dir_instalación* es el directorio de instalación del agente o agentes de supervisión.
2. Si desea desinstalar un agente de supervisión específico, especifique el nombre de script del agente y la opción de desinstalación donde *nombre* es el nombre de script del agente:
   - Linux AIX `./`*nombre*`-agent.sh uninstall`
   - Windows *nombre*`-agent.bat uninstall`

Para obtener una lista de los nombres de script de agente, consulte "Utilización de mandatos de agente" en la página 184.

Recuerde: Para el Monitoring Agent for Microsoft .NET, debe ejecutar el mandato con privilegios de administrador.

El agente de supervisión se ha desinstalado del sistema gestionado.

Si ha desinstalado todos los agentes de supervisión de forma individual, continúe para eliminar los archivos de la infraestructura. Consulte Qué hacer a continuación.

3. Si desea desinstalar todos los agentes de supervisión del sistema gestionado con una solicitud de confirmación, escriba el nombre del script y la opción uninstall_all:
   - Linux AIX `./smai-agent.sh uninstall_all`
   - Windows `smai-agent.bat uninstall_all`

   Se mostrará una solicitud de confirmación. Especifique 1 para continuar o 2 para cancelar.

   Todos los agentes de supervisión se han desinstalado del sistema o de la VM.
4. Linux AIX

   En Linux y UNIX, para forzar la desinstalación de todos los agentes de supervisión sin solicitudes de confirmación, escriba el nombre del script y la opción force uninstall all:

   ```
   ./smai-agent.sh uninstall_all force
   ```

Qué hacer a continuación

Para el Monitoring Agent for HTTP Server, después de desinstalar el agente, debe eliminar los archivos siguientes manualmente:

- `/tmp/khu_cps.properties`
- `/tmp/httpserver-disc.error`

En el Monitoring Agent for Python:

1. Suprima el archivo de configuración de Django `pyc` para asegurarse de que el archivo restaurado `pyc` de Django genera su binario.
2. Reinicie el servidor Apache para eliminar el middleware cargado en los procesos de Apache.

Para el Monitoring Agent for Ruby, desinstale el recopilador de datos de diagnóstico:

1. Vaya al directorio de inicio de la aplicación, abra su `Gemfile` y elimine la línea siguiente del archivo: `gem 'stacktracer'`
2. Reinicie la aplicación Ruby on Rails.
3. Desinstale el recopilador de datos de diagnóstico. Especifique: `gem uninstall` *`Gemfile`*
4. Elimine el directorio de tiempo de ejecución del recopilador de datos. La ubicación predeterminada de este directorio es *`dir_instalación`*`/install-images/kkm/dchome`

Para el Monitoring Agent for Microsoft .NET, complete estos pasos:

1. Elimine los archivos `dll` del recopilador de datos utilizando una de las opciones siguientes:
   - Rearranque el sistema operativo.
   - Intente suprimir el archivo *`dir_instalación`*`\qe\bin64\CorProfLog.dll`.

     Se mostrará un diálogo de `archivo en uso`, en el que se identifican los procesos de .NET que están actualmente en ejecución.
   - Reinicie todos los procesos de .NET.
2. Reinicie las aplicaciones .NET.

Agente de WebSphere Applications: Desconfiguración del recopilador de datos

Si desinstala el Agente de WebSphere Applications antes de desconfigurar el recopilador de datos, la desinstalación del agente no se realiza correctamente. Puede eliminar el recopilador de datos de una instancia del servidor de aplicaciones manualmente o utilizando el programa de utilidad interactivo, o el proceso de desconfiguración silenciosa.

Para instancias supervisadas con la supervisión de recursos de PMI, la desconfiguración no está disponible. La supervisión de los datos de PMI continúa mientras el servidor está disponible.

Desconfiguración interactiva del recopilador de datos

Si ya no desea que el recopilador de datos supervise una o más instancias de servidor de aplicaciones, puede desconfigurar el recopilador de datos para estas.

Antes de empezar

Para desconfigurar el recopilador de datos, utilice el ID de usuario de configuración del recopilador de datos, que es también el ID de usuario de instalación del servidor de aplicaciones. Compruebe que este ID de usuario tenga permisos de lectura y escritura sobre el directorio de inicio del recopilador de datos y sobre todos sus subdirectorios. El directorio de inicio del recopilador de datos es el siguiente, donde *dir_instalación* es el directorio de instalación de Agente de WebSphere Applications.

- Windows *dir_instal*\dchome\7.3.0.14.08
- Linux AIX *dir_instal*/yndchome/7.3.0.14.08

Acerca de esta tarea

El programa de utilidad de desconfiguración (`unconfig.sh` o `unconfig.bat`) es un programa de utilidad de línea de mandatos controlado por menús para desconfigurar el recopilador de datos.

Procedimiento

1. Inicie la sesión en el sistema con el ID de usuario utilizado para configurar el recopilador de datos.
2. Navegue al siguiente directorio `bin`:
   - Windows *dir_instalación*\dchome\7.3.0.14.08\bin
   - Linux AIX *dir_instalación*/yndchome/7.3.0.14.08/bin
3. Opcional: Establezca la ubicación del directorio de inicio Java antes de iniciar el programa de utilidad. Por ejemplo:

   Linux AIX
   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```

   Windows
   ```
   set JAVA_HOME=C:\Progra~1\IBM\WebSphere\AppServer80\java
   ```
4. Inicie el programa de utilidad de desconfiguración emitiendo el siguiente mandato:

   Linux AIX
   ```
   ./unconfig.sh
   ```

   Windows
   ```
   unconfig.bat
   ```
5. El programa de utilidad busca todas las instancias del servidor que están supervisadas por el recopilador de datos. Especifique el número que corresponde a la instancia de servidor de aplicaciones para desconfigurar la recopilación de datos o especifique un asterisco (`*`) para desconfigurar la recopilación de datos para todas las instancias de servidor de aplicaciones. Para especificar un subconjunto de servidores, especifique los números, separados por comas, que representan los servidores. Por ejemplo: `1,2,3`.

   Recuerde:

   - Para un entorno autónomo, las instancias de servidor de aplicaciones deben estar ejecutándose durante la configuración. (No es necesario que una instancia de WebSphere Application Server Liberty esté en ejecución).

- En un entorno de Network Deployment, el agente de nodo y el gestor de despliegue deben estar en ejecución.

6. El programa de utilidad le solicita que especifique si desea crear una copia de seguridad de la configuración de WebSphere Application Server. Especifique 1 para crear una copia de seguridad de la configuración actual. De lo contrario, especifique 2 y vaya al paso 8.
7. El programa de utilidad le solicita que especifique el directorio en el que se debe guardar la copia de seguridad de la configuración. Especifique un directorio en el que desea almacenar la copia de seguridad de la configuración o acepte el directorio predeterminado.

   El programa de utilidad muestra el nombre del directorio de inicio de WebSphere y el perfil de WebSphere para el que se ha creado una copia de seguridad.
8. El programa de utilidad indica si WebSphere Global Security está habilitada para el WebSphere Application perfil que ha especificado. Si la seguridad global no está habilitada, vaya al paso 10.
9. El programa de utilidad le solicita que especifique si se van a recuperar valores de seguridad de un archivo de propiedades de cliente. Especifique 1 para permitir que el programa de utilidad recupere el nombre de usuario y la contraseña del archivo de propiedades de cliente correspondiente y pasar al paso "10" en la página 155. En caso contrario, especifique 2 para indicar el nombre de usuario y la contraseña.

   El recopilador de datos se comunica con los Servicios administrativos de WebSphere utilizando RMI o el protocolo SOAP. Si la seguridad global está habilitada para un perfil, debe especificar el ID de usuario y la contraseña de un usuario que tenga autorización para iniciar sesión en la consola administrativa de IBM WebSphere Application Server para el perfil. O bien puede cifrar el nombre de usuario y la contraseña y almacenarlos en archivos de propiedades de cliente antes de configurar el recopilador de datos. Debe utilizar el archivo `sas.client.props` para una conexión RMI o el archivo `soap.client.props` para una conexión SOAP.

   Si ha seleccionado la opción para hacer copia de seguridad de la configuración actual de WebSphere, el programa de utilidad comienza a hacer una copia de seguridad de la configuración.
10. El programa de utilidad desconfigura el recopilador de datos para las instancias de servidor de aplicaciones especificadas. Se visualiza un mensaje de estado para indicar que el recopilador de datos se ha desconfigurado satisfactoriamente.
11. Una vez finalizada la desconfiguración del recopilador de datos, reinicie las instancias del servidor de aplicaciones.

    La configuración del recopilador de datos se aplica cuando se reinician las instancias de servidor de aplicaciones. La supervisión de recursos de PMI para la instancia del servidor sigue estando disponible.
12. Opcional: Si desea utilizar la supervisión de recursos para una instancia de servidor después de desconfigurar el recopilador de datos, reinicie el agente de supervisión ejecutando los mandatos siguientes:

    - Windows

      ```
      cd dir_instalación\bin
      was-agent.bat stop
      was-agent.bat start
      ```

    - Linux AIX

      ```
      cd dir_instalación/bin
      ./was-agent.sh
      stop
      ./was-agent.sh start
      ```

Resultados

El recopilador de datos se desconfigura para las instancias de servidor de aplicaciones especificadas.

Desconfiguración del recopilador de datos en modalidad silenciosa

Puede desconfigurar el recopilador de datos utilizando el programa de utilidad de desconfiguración en modalidad silenciosa.

Antes de empezar

Para desconfigurar el recopilador de datos, utilice el ID de usuario de configuración del recopilador de datos, que es también el ID de usuario de instalación del servidor de aplicaciones. Compruebe que este ID de usuario tenga permisos de lectura y escritura sobre el directorio de inicio del recopilador de datos y sobre todos sus subdirectorios. El directorio de inicio del recopilador de datos es el siguiente, donde *dir_instalación* es el directorio de instalación de Agente de WebSphere Applications.

- Windows *dir_instal*\dchome\7.3.0.14.08
- Linux AIX *dir_instal*/yndchome/7.3.0.14.08

Acerca de esta tarea

Al desconfigurar el recopilador de datos en modalidad silenciosa, primero se deben especificar las opciones de configuración en un archivo de propiedades. Un archivo de propiedades de ejemplo, `sample_silent_unconfig.txt`, viene empaquetado con el programa de utilidad de desconfiguración. El archivo está disponible en el directorio `bin` del directorio de inicio del recopilador de datos.

Procedimiento

1. Inicie la sesión en el sistema con el ID de usuario utilizado para configurar el recopilador de datos.
2. Especifique las opciones de configuración en el archivo `properties.txt`.

   Las siguientes propiedades están disponibles al desconfigurar el recopilador de datos en modalidad silenciosa:

   Valores de conexión de WebSphere Application Server

   was.wsadmin.connection.host
   Especifica el nombre del host al que se está conectando la herramienta wsadmin.

   Valores de seguridad global de WebSphere Application Server

   was.wsadmin.username
   Especifica el ID de un usuario con autorización para iniciar una sesión en la consola administrativa de IBM WebSphere Application Server. Este usuario debe tener el rol de agente en el servidor de aplicaciones.

   was.wsadmin.password
   Especifica la contraseña que corresponde al usuario especificado en la propiedad `was.wsadmin.username`.

   Valores de WebSphere Application Server

   was.appserver.profile.name
   Especifica el nombre del perfil del servidor de aplicaciones que desea desconfigurar.

   was.appserver.home
   Especifica el directorio de inicio de WebSphere Application Server.

   was.appserver.cell.name
   Especifica el nombre de célula de WebSphere Application Server.

   was.appserver.node.name
   Especifica el nombre de nodo de WebSphere Application Server.

   Copia de seguridad de la configuración de WebSphere Application Server

   was.backup.configuration
   Especifica si se debe realizar una copia de seguridad de la configuración actual del recopilador de datos de WebSphere Application Server antes de desconfigurar el recopilador de datos. Los valores válidos son `True` y `False`.

was.backup.configuration.dir
Especifica la ubicación del directorio de copia de seguridad.

Valores de la instancia de tiempo de ejecución de WebSphere Application Server

was.appserver.server.name
Especifica una instancia de servidor de aplicaciones dentro del perfil del servidor de aplicaciones para el que desea desconfigurar el recopilador de datos.

Consejo: El archivo de respuestas silencioso puede tener varias instancias de esta propiedad.

3. Acceda al directorio siguiente:
   - Windows *dir_instalación*\dchome\7.3.0.14.08\bin
   - Linux AIX *dir_instalación*/yndchome/7.3.0.14.08/bin
4. Ejecute el mandato siguiente:
   - Windows

     ```
     unconfig.bat -silent vía_acceso_archivo_silencioso
     ```

   - Linux AIX

     ```
     unconfig.sh -silent vía_acceso_archivo_silencioso
     ```

5. Una vez finalizada la desconfiguración del recopilador de datos, reinicie las instancias del servidor de aplicaciones.

   La configuración del recopilador de datos se aplica cuando se reinician las instancias de servidor de aplicaciones. La supervisión de recursos de PMI para la instancia del servidor sigue estando disponible.
6. Opcional: Si desea utilizar la supervisión de recursos para una instancia de servidor después de desconfigurar el recopilador de datos, reinicie el agente de supervisión ejecutando los mandatos siguientes:
   - Windows

     ```
     cd dir_instalación\bin
     was-agent.bat stop
     was-agent.bat start
     ```

   - Linux AIX

     ```
     cd dir_instalación/bin
     ./was-agent.sh
     stop
     ./was-agent.sh start
     ```

Eliminación manual de la configuración del recopilador de datos de una instancia del servidor de aplicaciones

Para eliminar manualmente la configuración de recopilador de datos de una instancia del servidor de aplicaciones, debe poder conectarse al servidor de aplicaciones utilizando la herramienta wsadmin. Esto es posible únicamente si está utilizando WebSphere Application Server Network Deployment y Deployment Manager está en ejecución. Si no se puede iniciar WebSphere application server, debe restaurar WebSphere application server a partir de la copia de seguridad realizada durante la ejecución del programa de utilidad de configuración.

Acerca de esta tarea

Puede eliminar manualmente la configuración del recopilador de datos de una instancia del servidor de aplicaciones si se cumple alguna de estas condiciones:

- En un entorno que no es de despliegue de red, ha añadido manualmente la configuración del recopilador de datos a la instancia de servidor de aplicaciones y desea desconfigurar la recopilación de datos. La instancia del servidor de aplicaciones debe estar en ejecución.
- En un entorno de despliegue de red, ha añadido manualmente la configuración del recopilador de datos a la instancia de servidor de aplicaciones y desea desconfigurar la recopilación de datos. El agente de nodo y el gestor de despliegue en el servidor de aplicaciones debe estar en ejecución.
- En un entorno de despliegue de red, ha configurado la instancia del servidor de aplicaciones para la recopilación de datos de forma manual y el servidor de aplicaciones no se puede iniciar. El agente de nodo y el gestor de despliegue en el servidor de aplicaciones debe estar en ejecución.

Si ha configurado una instancia del servidor de aplicaciones autónomo para la recopilación de datos, ya sea de forma manual o con el programa de utilidad de configuración o de migración, y el servidor de aplicaciones no se puede iniciar, debe restaurar la configuración de WebSphere Application Server con la configuración de copia de seguridad. Para obtener más información, consulte "Restauración de la configuración del servidor de aplicaciones a partir de una copia de seguridad" en la página 911.

Recuerde:

- Debe realizar cambios manuales en la configuración de WebSphere application server para los recopiladores de datos como el usuario administrativo de WebSphere.
- Los cambios manuales en WebSphere application server para la recopilación de datos debe realizarlos únicamente un administrador de WebSphere experimentado. Cualquier error en el cambio de configuración manual puede dar lugar a que el servidor de aplicaciones no se inicie.
- Si configura manualmente el recopilador de datos para supervisar las instancias de servidor de aplicaciones, no puede utilizar el programa de utilidad de desconfiguración para desconfigurar el recopilador de datos.

Procedimiento

Para eliminar manualmente la configuración del recopilador de datos, lleve a cabo el siguiente procedimiento:

1. Inicie la sesión en la consola de WebSphere Administration Server.
2. Pulse **Servidores**.
3. Expanda **Tipo de servidor** y seleccione **Servidores de aplicaciones WebSphere**.
4. Pulse en el nombre del servidor.
5. En la pestaña Configuración, vaya a **Infraestructura de servidor** > **Java y gestión de procesos** > **Definición de procesos** > **Máquina virtual Java** > **Propiedades adicionales: propiedades personalizadas**.
6. Elimine cualquiera de las siguientes propiedades personalizadas de JVM, si aparecen:
   - `am.home`
   - `ITCAM.DC.ENABLED`
   - `TEMAGCCollector.gclog.path`
   - `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild`
   - `com.ibm.tivoli.jiti.injector.ProbeInjectorManagerChain. primaryInjectorFile`
7. Identifique los argumentos de JVM que se han añadido para el recopilador de datos.
   a) En el panel de navegación, pulse **Entorno** > **Variables de WebSphere**.
   b) Si ha configurado manualmente el servidor de aplicaciones para la recopilación de datos, localice los argumentos de JVM que ha añadido manualmente.

      Si ha configurado el servidor de aplicaciones para la recopilación de datos con los programas de utilidad de configuración, compare los valores de los argumentos **`AM_OLD_ARGS`** y **`AM_CONFIG_JVM_ARGS`** para determinar qué argumentos añadió el programa de utilidad de configuración.
8. Pulse **Servidor** > **Servidor de aplicaciones** y seleccione el nombre de servidor adecuado.

9. En la pestaña Configuración, vaya a **Infraestructura de servidor** > **Java y gestión de proceso** > **Definición de procesos** > **Máquina virtual Java**.
10. En el campo **Argumentos de JVM genéricos**, elimine los argumentos de JVM que se han identificado en el paso 7 para el recopilador de datos.
11. Pulse **Aplicar** o **Aceptar**.
12. En el recuadro de diálogo **Mensajes**, pulse **Guardar**.
13. En el recuadro de diálogo **Guardar en configuración maestra**, realice uno de los pasos siguientes:
    - Si está en un entorno de despliegue de red, asegúrese de que el recuadro de selección**Sincronizar cambios con nodos** está seleccionado y, a continuación, pulse **Guardar**.
    - Si no está en un entorno de despliegue de red, pulse **Guardar**.
14. Elimine las entradas de entorno que se añadieron para el recopilador de datos.
    a) En la pestaña Configuración, vaya a **Infraestructura de servidor** > **Java y gestión de procesos** > **Definición de procesos** > **Entradas de entorno**.
    b) En función del sistema operativo, suprima la siguiente entrada de entorno:
       - UNIX **LIBPATH**
       - Linux **LD_LIBRARY_PATH**
       - Windows **PATH**
    c) Elimine la entrada de entorno **NLSPATH**.
15. Pulse **Aplicar** o **Aceptar**.
16. En el recuadro de diálogo **Mensajes**, pulse **Guardar**.
17. En el recuadro de diálogo **Guardar en configuración maestra**, realice uno de los pasos siguientes:
    - Si está en un entorno de despliegue de red, asegúrese de que el recuadro de selección **Sincronizar cambios con nodos** está seleccionado y, a continuación, pulse **Guardar**.
    - Si no está en un entorno de despliegue de red, pulse **Guardar**.
18. En el panel de navegación, pulse **Entorno** > **Variables de WebSphere**.
19. Suprima las siguientes variables:
    - **AM_CONFIG_JVM_ARGS**
    - **AM_OLD_JVM_ARGS**
    - **ITCAMDCHOME**
    - **ITCAMDCVERSION**
20. En el recuadro de diálogo **Mensajes**, pulse **Guardar**.
21. En el recuadro de diálogo **Guardar en configuración maestra**, realice uno de los pasos siguientes:
    - Si está en un entorno de despliegue de red, asegúrese de que el recuadro de selección **Sincronizar cambios con nodos** está seleccionado y, a continuación, pulse **Guardar**.
    - Si no está en un entorno de despliegue de red, pulse **Guardar**.
22. Si ha configurado la instancia de servidor para la recopilación de datos con la herramienta de configuración del recopilador de datos, en lugar de manualmente, realice los pasos siguientes:
    a) Vaya al directorio *dir_inicio_dc*/runtime.
    b) Cambie el nombre del archivo $profile.$cell.$node.$server.input.properties por $profile.$cell.$node.$server.input.properties.bak.
23. Si va a eliminar manualmente la configuración del recopilador de datos de todas las instancias del servidor de aplicaciones de un perfil, siga estos pasos:
    a) Vaya al directorio $appserverhome/bin.
    b) Ejecute el mandato **osgiCfgInit.sh/bat -all** en los sistemas Windows o el mandato **osgiCfgInit.sh -all** en los sistemas UNIX y Linux.
24. Reinicie la instancia del servidor de aplicaciones supervisada por el recopilador de datos.

Desconfiguración manual del recopilador de datos
Tras configurar manualmente el recopilador de datos para el Agente de WebSphere Applications, para eliminar la recopilación de datos del servidor de aplicaciones configurado, debe desconfigurar manualmente el recopilador de datos.

Acerca de esta tarea

El procedimiento siguiente sólo es aplicable tras configurar manualmente el recopilador de datos siguiendo las instrucciones de la sección "Configuración manual del recopilador de datos si fallan los programas de utilidad de configuración" en la página 886. Si ha utilizado los programas de utilidad de configuración para configurar el recopilador de datos, también debe utilizar el programa de utilidad de desconfiguración para desconfigurar el recopilador de datos. Para obtener instrucciones, consulte las secciones "Desconfiguración interactiva del recopilador de datos" en la página 154 o "Desconfiguración del recopilador de datos en modalidad silenciosa" en la página 156.

Procedimiento

- Para desconfigurar manualmente el recopilador de datos de WebSphere Application Server, consulte "Desconfiguración manual del recopilador de datos para WebSphere Application Server tradicional" en la página 160.
- Para desconfigurar manualmente el recopilador de datos de Liberty Server, consulte "Desconfiguración manual del recopilador de datos para WebSphere Application Server Liberty" en la página 161.

Desconfiguración manual del recopilador de datos para WebSphere Application Server tradicional

Procedimiento

1. Inicie la sesión en la consola administrativa de WebSphere como administrador.
2. En el panel de navegación, pulse **Servidores**, expanda **Tipo de servidor** y seleccione **Servidores de aplicaciones WebSphere**.
3. Pulse el nombre del servidor de aplicaciones.
4. En la sección **Infraestructura de servidor** de la pestaña Configuración, expanda **Máquina virtual Java** y pulse **Definición de procesos**.
5. En la sección **Propiedades adicionales**, pulse **Máquina virtual Java**.
6. En el campo **Argumentos de JVM genéricos**, elimine las siguientes entradas del contenido.

```
-agentlib:am_ibm_16=${WAS_SERVER_NAME} -Xbootclasspath/p:${ITCAMDCHOME}/
toolkit/lib/bcm-bootstrap.jar -Djava.security.policy=${ITCAMDCHOME}/itcamdc/
etc/datacollector.policy -verbosegc
```

7. Pulse **Aceptar** y pulse **Guardar**. En el recuadro de diálogo Guardar en configuración maestra, realice los pasos siguientes:
   - Si está en un entorno de despliegue de red, asegúrese de que **Sincronizar cambios con nodos** está seleccionado y luego pulse **Guardar**.
   - Si no está en un entorno de despliegue de red, pulse **Guardar**.
8. En el panel de navegación, pulse **Servidores**, expanda **Tipos de servidores**, pulse **Servidores de aplicaciones WebSphere** y pulse el nombre del servidor.
9. En la pestaña Configuración, vaya a **Infraestructura de servidor** > **Java y gestión de procesos** > **Definición de procesos** > **Entradas de entorno**.
10. Dependiendo del sistema operativo, la plataforma de hardware y la JVM del servidor de aplicaciones, elimine la siguiente entrada de entorno.
    - UNIX LIBPATH
    - Linux LD_LIBRARY_PATH
    - Windows PATH

11. En el panel de navegación, pulse **Entorno** > **Variables de WebSphere**.
12. Elimine la variable *ITCAMDCHOME* si existe.
13. Pulse **Aceptar** y pulse **Guardar**. En el recuadro de diálogo Guardar en configuración maestra, realice los pasos siguientes:
    - Si está en un entorno de despliegue de red, asegúrese de que **Sincronizar cambios con nodos** está seleccionado y luego pulse **Guardar**.
    - Si no está en un entorno de despliegue de red, pulse **Guardar**.
14. Reinicie la instancia del servidor de aplicaciones.
15. Vaya al directorio `runtime` del directorio de instalación del agente y elimine el archivo *nombre_perfil.nombre_célula.nombre_nodo.nombre_servidor*`.manual.input.properties` file.
    - Linux AIX *dir_instalación*`/yndchome/7.3.0.14.08/runtime/`*nombre_perfil.nombre_célula.nombre_nodo.nombre_servidor*`.manual.input.properties`
    - Windows *dir_instalación*`\dchome\7.3.0.14.08\runtime\`*nombre_perfil.nombre_célula.nombre_nodo.nombre_servidor*`.manual.input.properties`

Desconfiguración manual del recopilador de datos para WebSphere Application Server Liberty

Procedimiento

1. Navegue el directorio del servidor Liberty y abra el archivo `jvm.options` del directorio *nombre_servidor* del directorio de instalación del servidor Liberty. Por ejemplo, `/opt/ibm/wlp/usr/servers/defaultServer`.
2. Elimine los parámetros siguientes del archivo `jvm.options`.

```
-agentlib:am_ibm_16=nombre_servidor
–Xbootclasspath/p:inicio_dc/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=inicio_dc/itcamdc/etc/datacollector.policy
-verbosegc
```

   donde *nombre_servidor* es el nombre del servidor Liberty, e *inicio_dc* es el directorio de inicio del recopilador de datos.
3. Abra el archivo `server.xml` y elimine las líneas siguientes:

```
<feature>webProfile-7.0</feature>
<feature>monitor-1.0</feature>
<feature>usr:itcam-730.140</feature>
```

4. Abra el archivo `server.env` y elimine el valor de entrada siguiente de la entrada de entorno en función del sistema operativo:

Tabla 8. Entrada de entorno

Plataforma	Nombre de entrada de entorno	Valor de entrada de entorno
AIX R6.1 (JVM de 64 bits)	LIBPATH	`/lib:`*inicio_dc*`/toolkit/lib/aix536`
AIX R7.1 (JVM de 64 bits)	LIBPATH	`/lib:`*inicio_dc*`/toolkit/lib/aix536`
Solaris 10 (JVM de 64 bits)	LIBPATH	`/lib:`*inicio_dc*`/toolkit/lib/sol296`
Solaris 11 (JVM de 64 bits)	LIBPATH	`/lib:`*inicio_dc*`/toolkit/lib/sol296`

Tabla 8. Entrada de entorno (continuación)		
Plataforma	**Nombre de entrada de entorno**	**Valor de entrada de entorno**
Linux x86_64 R2.6 (JVM de 64 bits)	LD_LIBRARY_PATH	/lib:*inicio_dc*/toolkit/lib/lx8266
Linux Intel R2.6 (JVM de 32 bits)	LD_LIBRARY_PATH	/lib:*inicio_dc*/toolkit/lib/li6263
Windows (JVM de 32 bits)	PATH	/lib;*inicio_dc*/toolkit/lib/win32
Windows (JVM de 64 bits)	PATH	/lib;*inicio_dc*/toolkit/lib/win64

5. Reinicie el servidor Liberty.
6. Vaya al directorio `runtime` del directorio de instalación del Agente de WebSphere Applications y elimine el archivo *nombre_célula*.*nombre_nodo*.*nombre_servidor*.manual.input.properties
   - Linux AIX *dir_instalación*/yndchome/7.3.0.14.08/runtime/*nombre_célula*.*nombre_nodo*.*nombre_servidor*.manual.input.properties
   - Windows *dir_instalación*\dchome\7.3.0.14.08\runtime*nombre_célula*.*nombre_nodo*.*nombre_servidor*.manual.input.properties

Agente de Node.js: eliminación del plug-in de supervisión

Antes de desinstalar el Agente de Node.js, debe eliminar el plug-in de supervisión de la aplicación Node.js.

Procedimiento

1. Eliminar plug-ins de recopilador de datos del principio del archivo de aplicación Node.js.
   - Si actualiza el Agente de Node.js de V01.00.12.00 a V01.00.13.00, siga este procedimiento:
     - Si ha habilitado la recopilación de datos de recurso, elimine la línea siguiente del principio del archivo de aplicación de Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_index.js');
       ```

       donde *KNJ_NPM_LIB_LOCATION* es el directorio a la carpeta `lib` del directorio de instalación global del paquete npm. El directorio predeterminado es `/usr/local/lib`.
     - Si ha habilitado la recopilación de datos de recurso y la recopilación de datos de diagnóstico detallado, elimine la línea siguiente del principio del archivo de aplicación Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_deepdive.js');
       ```

     - Si ha habilitado la recopilación de datos de recurso, la recopilación de datos de diagnóstico detallado y la recopilación de rastreos de método, elimine la línea siguiente del principio del archivo de aplicación Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_methodtrace.js');
       ```

   - Si actualiza el Agente de Node.js de V01.00.10.00 a V01.00.13.00, siga este procedimiento:
     - Si habilitó la recopilación de datos de recurso, elimine la línea siguiente del principio del archivo de aplicación de Node.js.

       ```
       require('dir_instalación/lx8266/nj/bin/plugin/knj_index.js');
       ```

       , donde *dir_instalación* es el directorio de instalación de Agente de Node.js.

– Si ha habilitado la recopilación de datos de recurso y la recopilación de datos de diagnóstico detallado, elimine la línea siguiente del principio del archivo de aplicación Node.js.

```
require('dir_instalación/lx8266/nj/bin/plugin/knj_deepdive.js');
```

– Si ha habilitado la recopilación de datos de recurso, la recopilación de datos de diagnóstico detallado y la recopilación de rastreos de método, elimine la línea siguiente del principio del archivo de aplicación Node.js.

```
require('dir_instalación/lx8266/nj/bin/plugin/knj_methodtrace.js');
```

2. Reinicie la aplicación Node.js para inhabilitar los plug-in de recopilador de datos.
   - Si la versión del Agente de Node.js actual es V01.00.10.00, hasta ahora los plug-ins de recopilador de datos se han eliminado satisfactoriamente.
   - Si la versión del Agente de Node.js actual es V01.00.12.00, vaya al paso siguiente.
3. Ejecute el mandato `./uninstall.sh` desde el directorio *dir_instalación*`/lx8266/nj/bin` para eliminar los valores de agente anteriores.

Qué hacer a continuación

Para obtener más información sobre cómo desinstalar el Agente de Node.js, consulte "Desinstalación de los agentes" en la página 151.

Agente de Microsoft .NET: eliminación del recopilador de datos .NET

Antes de desinstalar Agente de Microsoft .NET, debe eliminar el recopilador de datos .NET de las aplicaciones .NET.

Procedimiento

1. Anule el registro del recopilador de datos.
   Como administrador, escriba:

   ```
   cd dir_instalación\qe\bin configdc unregisterdc
   ```

   Donde *dir_instalación* es el directorio de instalación del Agente de Microsoft .NET.
2. Detenga todas las aplicaciones .NET para inhabilitar el recopilador de datos.
   Especifique `net stop was /y`
3. Para garantizar la limpieza completa de .NET Data Collector tras la desinstalación, siga estos pasos:
   a) En el indicador de mandatos, vaya al directorio `< APM_HOME>\qe\bin`.
   b) Ejecute el archivo `ProcListCaller.bat`.
   c) Verifique el archivo de registro `CorProfAttach.Log` en el directorio `<APM_HOME>\qe\logs`. El archivo de registro lista los procesos a los que se conecta el componente de perfilador .NET DC.
   d) Antes de desinstalar el agente, detenga los procesos del archivo `CorProfAttach.Log`.
   e) Si no se listan procesos, continúe con la desinstalación del agente.

Qué hacer a continuación

Desinstale el Agente de Microsoft .NET. Consulte "Desinstalación de los agentes" en la página 151.

Capítulo 7. Configuración del entorno

Si hay que configurar el agente de supervisión o se desean revisar los valores predeterminados de un agente, siga los pasos proporcionados para el agente.

Temas comunes

Algunos temas son comunes cuando se configuran agentes y recopiladores de datos.

Conectividad de red

Para asegurarse de que se han establecido las comunicaciones del servidor del agente, pruebe la conectividad del sistema con el Servidor de Cloud APM.

Para validar las comunicaciones, pruebe la conectividad al centro de datos de Cloud APM. Para asegurarse de que las reglas de cortafuegos permiten tráfico de retorno desde tres direcciones IP específicas y el puerto 443, busque las tres direcciones IP del centro de datos que necesita para verificar la conexión. Para obtener más información, consulte Data Center IP addresses (SaaS only) en Application Performance Management Developer Center. Compruebe que los agentes pueden conectarse a estas tres direcciones IP utilizando el mandato **openssl**. Para obtener más información sobre el uso del mandato **openssl**, consulte la sección Configuración de agentes para la comunicación mediante un proxy directo. Si los agentes no pueden conectarse, póngase en contacto con el equipo local de TI. Sus técnicos pueden ajustar las reglas de cortafuegos, habilitar el puerto 443 y habilitar el tráfico TLS 1.2 de los servidores, o configurar un servidor proxy para conectarse al Servidor de Cloud APM.

Si las reglas de cortafuegos no permiten establecer conexiones HTTPS transparentes de salida a host externos, puede configurar los agentes para enviar el tráfico a un proxy directo. Para obtener más información, consulte “Configuración de agentes para la comunicación mediante un proxy directo” en la página 165.

Conectividad del navegador

Para comprobar la conectividad del navegador con la Consola de Cloud APM, localice el URL de **Launch**, que le proporcionó IBM cuando se suministró la suscripción. También puede iniciar sesión en su cuenta e iniciar la consola. Inicie sesión en la página **Productos y servicios** (http://ibm.biz/my-prodsvcs) con sus detalles de suscripción de IBM Marketplace. Pulse **Iniciar** para iniciar la consola y visualice el URL, por ejemplo: `8b68ba1b9.agents.na.apm.ibmserviceengage.com`. Verifique que puede utilizar el URL para iniciar sesión en la consola.

Comunicación segura

La comunicación segura entre los agentes y el Servidor de Cloud APM requiere TLS 1.2.

La comunicación entre los agentes y el Servidor de Cloud APM en la nube de IBM utiliza HTTPS con TLS 1.2 y los paquetes de cifrado FIPS Suite-B. Se utilizan los cifrados siguientes:

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

La comunicación entre el navegador y el Servidor de Cloud APM también requiere TLS 1.2. En algunos navegadores, TLS 1.2 no está habilitado de forma predeterminada y debe habilitarse manualmente.

Configuración de agentes para la comunicación mediante un proxy directo

Si las reglas de cortafuegos no permiten establecer conexiones HTTPS transparentes de salida a host externos, debe configurar agentes de supervisión de IBM para enviar el tráfico a un proxy directo. Edite la variable de entorno KDH_FORWARDPROXY para configurar los agentes para comunicar a través del proxy directo.

Antes de empezar

Para determinar la dirección IP del centro de datos de Cloud APM al que se conectan sus agentes, consulte Direcciones IP de centro de datos (APM Developer Center). A continuación, ajuste las reglas del cortafuegos para permitir que se envíen solicitudes a esas direcciones IP desde su proxy directo.

Puede utilizar el mandato **openssl** para comprobar si el sistema donde están instalados sus agentes tiene conectividad a los servidores de centro de datos de Cloud APM. También puede utilizar el mandato **openssl** para comprobar si la red da soporte a las suites de cifrado utilizadas por Cloud APM. Si los resultados del mandato **openssl** indican que el sistema no puede conectarse, es posible que tenga que configurar un proxy directo. Si los resultados del mandato indican que el certificado del Servidor de Cloud APM no puede obtenerse, colabore con su equipo de red para determinar por qué las suites de cifrado necesarias no están soportadas. Para conocer la lista de suites de cifrado utilizadas por Cloud APM, consulte "Comunicación segura" en la página 165.

Ejecute el mandato **openssl** tal como se muestra en el ejemplo siguiente:

```
echo quit | openssl s_client
-state -connect <nombre-dominio>:443
-tls1_2 -cipher
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384
```

donde *nombre-dominio* es el nombre de dominio de la suscripción de Cloud APM (por ejemplo: `8b68ba1b9.agents.na.apm.ibmserviceengage.com`).

Para determinar el nombre de dominio para su suscripción, complete los pasos siguientes:

1. Abra el archivo de configuración del entorno de agente en un editor de texto:

   Linux AIX `/opt/ibm/apm/agent/config/global.environment`

   Windows `dir_instalación\TMAITM6_x64\K`*pc*`ENV` para sistemas Windows de 64 bits y `dir_instalación\TMAITM6\K`*pc*`ENV` para sistemas Windows de 32 bits, donde *pc* es el código de producto del agente.

   Para ver una lista de códigos de productos, consulte el "Utilización de mandatos de agente" en la página 184.
2. Localice la variable *IRA_ASF_SERVER_URL*. El valor tiene la forma: `https://nombre-dominio/ccm/asf/solicitud`. Utilice la parte de nombre de dominio del valor con el mandato **openssl**.

Si la conexión es satisfactoria, se visualizarán mensajes similares a los del ejemplo siguiente:

```
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=2 C = US, O = IBM Service Engage,
CN = ca_ec_384.ibmserviceengage.com
verify error:num=19:self signed certificate in certificate chain
verify return:0
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server key exchange A
SSL_connect:SSLv3 read server certificate request A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client certificate A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read finished A
---
Certificate chain
0 s:/C=US/O=IBM Service Engage/OU=Application Performance
```

```
Management/CN=*.agents.na.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN =ca_ec_384.apm.ibmserviceengage.com
1 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
2 s:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICkjCCAhegAwIBAgIIXlr284nLPaMwDAYIKoZIzj0EAwMFADCBhDELMAkGA1UE
BgwCVVMxGzAZBgNVBAoMEklCTSBTZXJ2aWNlIEVuZ2FnZTErMCkGA1UECwwiQXBw
bGljYXRpb24gUGVyZm9ybWFuY2UgTWFuYWdlbWVudDErMCkGA1UEAwwiY2FfZWNf
Mzg0LmFwbS5pYm1zZXJ2aWNlZW5nYWdlLmNvbTAeFw0xMzEyMDIxNjM2MDlaFw0y
MzEyMDExNjM2MDlaMIGGMQswCQYDVQQGDAJVUzEbMBkGA1UECgwSSUJNIFNlcnZp
Y2UgRW5nYWdlMSswKQYDVQQLDCJBcHBsaWNhdGlvbiBQZXJmb3JtYW5jZSBNYW5h
Z2VtZW50MS0wKwYDVQQDDCQqLmFnZW50cy5uYS5hcG0uaWJtc2VydmljZWVuZ2Fn
ZS5jb20wdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAQmrGoCkAMoNAC3F6MIo1zR8fcO
mczYXtUux2bhlOibn3jQdxamhDR91nr2RBerGjMIITKNXd2MaOr3b6m8euk1BAL3
KsbN9lqvw94kXg0BTO1IHAcdsZQB+AuEVVhmDVGjUDBOMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU/zpE5TOnQ8LSuvbSWRfpbiGea08wHQYDVR0OBBYEFHL0At4O
GUdcOHVGg4Tfo4hl7LLGMAwGCCqGSM49BAMDBQADZwAwZAIwDWPHo5I04ZFVrkfk
St6gwH2UNF37jBscRN1lOE4SIwezZAqVs42BNMkWRjJBgiHzAjBm4m3zOjsXzNL8
+u8ALjQQCpBDT6dUHujzY5CRxG0xEHi5IXsXf4QwbctnjjvTeYA=
-----END CERTIFICATE-----
subject=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
issuer=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
---
Acceptable client certificate CA names
/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert
Global Root CA/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
Server Temp Key: ECDH, prime256v1, 256 bits
---
SSL handshake has read 2659 bytes and written 261 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-ECDSA-AES128-GCM-SHA256
Server public key is 384 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1.2
Cipher : ECDHE-ECDSA-AES128-GCM-SHA256
Session-ID:
A18C31D0B45A1166357C917E1CFCD86A9FBEDB4A0EB768EF5390AC28C95CB7EF
Session-ID-ctx:
Master-Key:
252B8FE2731E51AC0B79A27C7BED33CA8B15AF4CFD015C98DBACA46EA01DC40B
9E6B56E62E0F332FF6B56266B5ADD7B0
Key-Arg : None
Krb5 Principal: None
```

```
PSK identity: None
PSK identity hint: None
Start Time: 1510772474
Timeout : 7200 (sec)
Verify return code: 19 (self signed certificate in certificate chain)
---
DONE
SSL3 alert write:warning:close notify
```

Si el sistema no tiene conectividad con el Servidor de Cloud APM, se visualizarán mensajes similares a los del ejemplo siguiente:

```
getaddrinfo: Name or service not known
connect:errno=2
```

Si el sistema no puede obtener el certificado de servidor porque las suites de cifrado están bloqueadas en algún punto de la red, se visualizarán mensajes similares a los del ejemplo siguiente:

```
SSL_connect:failed
---
no peer certificate available
---
No client certificate CA names sent
```

Acerca de esta tarea

Al utilizar un proxy directo, el agente abre primero una conexión TCP con el proxy. El agente envía una solicitud de HTTP CONNECT y el URL del punto final de destino (Servidor de Cloud APM) al proxy directo. A continuación, el proxy directo establece una conexión TCP con el punto final de destino y configura una sesión de tunelado HTTPS entre el agente y el Servidor de Cloud APM.

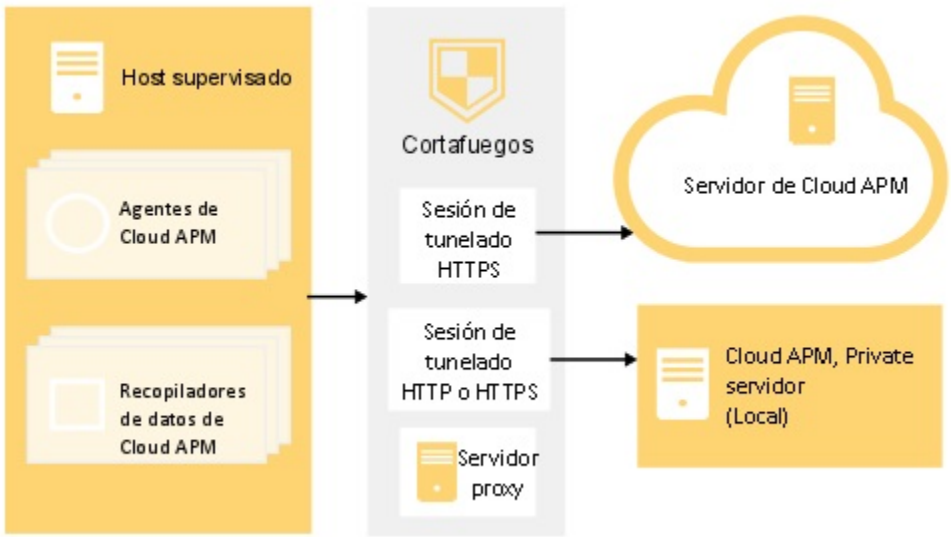


Figura 1. Diagrama de conexión para la utilización de un proxy directo

El agente de supervisión no soporta proxies de autenticación, lo que significa que el agente no soporta el inicio de la sesión en un proxy directo mediante un ID de usuario y una contraseña de proxy configurado.

Procedimiento

1. Abra el archivo de configuración del entorno de agente en un editor de texto:

   Linux AIX Archivo *dir_instalación*`/config/global.environment`, donde *dir_instalación* es el directorio de inicio de instalación de los agentes. El archivo `global.environment` configura todos los agentes en el directorio de instalación.

Los valores personalizados del archivo `.global.environment` se pierden después de la actualización del agente. Para conservar los valores, realice los cambios de configuración en los archivos `global.environment`. La actualización del agente no sobrescribe los valores de este archivo.

Windows Archivo *dir_instalación*\TMAITM6_x64\K*pc*ENV para agentes de 64 bits y *dir_instalación*\TMAITM6\K*pc*ENV para agentes de 32 bits, donde *pc* es el código de producto del agente. Configure el archivo K*pc*ENV para cada agente.

Para ver una lista de códigos de productos, consulte el "Utilización de mandatos de agente" en la página 184.

2. Edite la variable de entorno KDH_FORWARDPROXY para especificar la dirección de proxy y el puerto:

```
KDH_FORWARDPROXY=http://dirección-proxy:número-puerto-proxy
```

Por ejemplo:

```
KDH_FORWARDPROXY=http://HostA:8085
```

3. Reinicie el agente para implementar los cambios. Consulte "Utilización de mandatos de agente" en la página 184.

Configuración de recopiladores de datos para la comunicación mediante un proxy directo

Si las reglas de cortafuegos no permiten establecer conexiones HTTPS transparentes de salida a host externos, puede configurar recopiladores de datos para enviar el tráfico a un proxy directo. Edite la variable de entorno APM_GW_PROXY_CONNECTION para configurar recopiladores de datos para comunicar a través del proxy directo.

Antes de empezar

Para determinar la dirección IP del centro de datos de Cloud APM al que se conectan sus recopiladores de datos, consulte Direcciones IP de centro de datos (APM Developer Center). A continuación, ajuste las reglas del cortafuegos para permitir que se envíen solicitudes a esas direcciones IP desde su proxy directo.

Puede utilizar el mandato **openssl** para comprobar si el sistema donde están instalados sus recopiladores de datos tiene conectividad a los servidores de centro de datos de Cloud APM. También puede comprobar si la red da soporte a las suites de cifrado utilizadas por Cloud APM. Si los resultados del mandato **openssl** indican que el sistema no puede conectarse, es posible que tenga que configurar un proxy directo. Si los resultados del mandato indican que el certificado del Servidor de Cloud APM no puede obtenerse, colabore con su equipo de red para determinar por qué las suites de cifrado necesarias no están soportadas. Para conocer la lista de suites de cifrado utilizadas por Cloud APM, consulte "Comunicación segura" en la página 165.

Ejecute el mandato **openssl** tal como se muestra en el ejemplo siguiente:

```
echo quit | openssl s_client
-state -connect <nombre-dominio>:443
-tls1_2 -cipher
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384
```

donde *nombre-dominio* es el nombre de dominio de su suscripción de Cloud APM.

Para determinar el nombre de dominio para su suscripción, consulte "Configuración de agentes para la comunicación mediante un proxy directo" en la página 165.

Si la conexión es satisfactoria, se visualizarán mensajes similares a los del ejemplo siguiente:

```
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=2 C = US, O = IBM Service Engage,
CN = ca_ec_384.ibmserviceengage.com
verify error:num=19:self signed certificate in certificate chain
```

```
verify return:0
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server key exchange A
SSL_connect:SSLv3 read server certificate request A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client certificate A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read finished A
---
Certificate chain
0 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN =ca_ec_384.apm.ibmserviceengage.com
1 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
2 s:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICkjCCAhegAwIBAgIIXlr284nLPaMwDAYIKoZIzj0EAwMFADCBhDELMAkGA1UE
BgwCVVMxGzAZBgNVBAoMEklCTSBTZXJ2aWNlIEVuZ2FnZTErMCkGA1UECwwiQXBw
bGljYXRpb24gUGVyZm9ybWFuY2UgTWFuYWdlbWVudDErMCkGA1UEAwwiY2FfZWNf
Mzg0LmFwbS5pYm1zZXJ2aWNlZW5nYWdlLmNvbTAeFw0xMzEyMDIxNjM2MDlaFw0y
MzEyMDExNjM2MDlaMIGGMQswCQYDVQQGDAJVUzEbMBkGA1UECgwSSUJNIFNlcnZp
Y2UgRW5nYWdlMSswKQYDVQQLDCJBcHBsaWNhdGlvbiBQZXJmb3JtYW5jZSBNYW5h
Z2VtZW50MS0wKwYDVQQDDCQqLmFnZW50cy5uYS5hcG0uaWJtc2VydmljZWVuZ2Fn
ZS5jb20wdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAQmrGoCkAMoNAC3F6MIo1zR8fcO
mczYXtUux2bhlOibn3jQdxamhDR91nr2RBerGjMIITKNXd2MaOr3b6m8euk1BAL3
KsbN9lqvw94kXg0BTO1IHAcdsZQB+AuEVVhmDVGjUDBOMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU/zpE5TOnQ8LSuvbSWRfpbiGea08wHQYDVR0OBBYEFHL0At4O
GUdcOHVGg4Tfo4hl7LLGMAwGCCqGSM49BAMDBQADZwAwZAIwDWPHo5I04ZFVrkfk
St6gwH2UNF37jBscRN1lOE4SIwezZAqVs42BNMkWRjJBgiHzAjBm4m3zOjsXzNL8
+u8ALjQQCpBDT6dUHujzY5CRxG0xEHi5IXsXf4QwbctnjjvTeYA=
-----END CERTIFICATE-----
subject=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
issuer=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
---
Acceptable client certificate CA names
/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert
Global Root CA/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
Server Temp Key: ECDH, prime256v1, 256 bits
---
SSL handshake has read 2659 bytes and written 261 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-ECDSA-AES128-GCM-SHA256
Server public key is 384 bit
```

```
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1.2
Cipher : ECDHE-ECDSA-AES128-GCM-SHA256
Session-ID:
A18C31D0B45A1166357C917E1CFCD86A9FBEDB4A0EB768EF5390AC28C95CB7EF
Session-ID-ctx:
Master-Key:
252B8FE2731E51AC0B79A27C7BED33CA8B15AF4CFD015C98DBACA46EA01DC40B
9E6B56E62E0F332FF6B56266B5ADD7B0
Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1510772474
Timeout : 7200 (sec)
Verify return code: 19 (self signed certificate in certificate chain)
---
DONE
SSL3 alert write:warning:close notify
```

Si el sistema no tiene conectividad con el Servidor de Cloud APM, se visualizarán mensajes similares a los del ejemplo siguiente:

```
getaddrinfo: Name or service not known
connect:errno=2
```

Si el sistema no puede obtener el certificado de servidor porque las suites de cifrado están bloqueadas en algún punto de la red, se visualizarán mensajes similares a los del ejemplo siguiente:

```
SSL_connect:failed
---
no peer certificate available
---
No client certificate CA names sent
```

Acerca de esta tarea

Al utilizar un proxy directo, el recopilador de datos abre primero una conexión TCP con el proxy. El recopilador de datos envía una solicitud de conexión y el URL del punto final de destino (servidor Servidor de Cloud APM) al proxy directo. A continuación, el proxy directo establece una conexión TCP con el punto final de destino y configura una sesión de tunelado HTTPS entre el recopilador de datos y el servidor Servidor de Cloud APM.

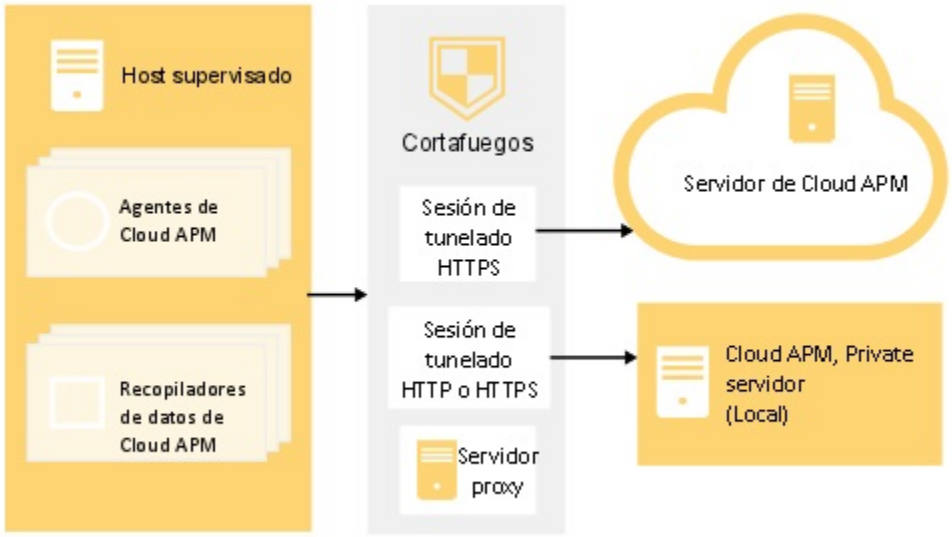


Figura 2. Diagrama de conexión para la utilización de un proxy directo

Algunos recopiladores de datos dan soporte a proxies de autenticación, por ejemplo los recopiladores de datos de Node.js y Liberty. Estos recopiladores de datos permiten iniciar la sesión en un proxy directo pero utilizan un ID de usuario y una contraseña de proxy configurados.

Procedimiento

1. Para configurar la comunicación de proxy directo para recopiladores de datos de Python, siga uno de estos pasos:
   - Abra el archivo de propiedades del recopilador de datos `<inicio rd>/config.properties` en un editor de texto, donde *<inicio rd>* es el directorio de inicio de instalación de los recopiladores de datos, por ejemplo `/usr/lib/python2.7/site-packages/ibm_python_dc`. Actualice la variable de con el host y el número de puerto del proxy, por ejemplo `APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085`. La edición de la variable de este archivo afecta a todas las aplicaciones con el recopilador de datos de Python habilitado.

     Nota: Para configurar la comunicación de proxy directo para una sola aplicación, copie el archivo `<inicio rd>/config.properties` en el directorio de la aplicación. Actualice la variable en el directorio de la aplicación.
   - Ejecute el mandato siguiente en sistemas Linux:

     ```
     export APM_GW_PROXY_CONNECTION =http://<host proxy http>:<puerto proxy http>
     ```

     Por ejemplo,

     ```
     export APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085
     ```
2. Para configurar la comunicación de proxy directo para recopiladores de datos de Node.js, siga uno de estos pasos:
   - Ejecute el mandato siguiente en sistemas Linux:

     ```
     export APM_GW_PROXY_CONNECTION =http://<host proxy http>:<puerto proxy http>
     ```

     Por ejemplo,

     ```
     export APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085
     ```
   - Si se necesita un nombre de usuario y una contraseña par acceder al servidor de proxy directo para los recopiladores de datos de Node.js, ejecute el mandato siguiente en sistemas Linux:

```
export APM_GW_PROXY_CONNECTION =http://<usuario proxy http>:
<contraseña proxy http>@<host proxy http>:<puerto proxy http>
```

Por ejemplo,

```
export APM_GW_PROXY_CONNECTION =http://Joe:passw0rd@9.181.138.247:8085
```

3. Para configurar la comunicación de proxy directo para recopiladores de datos de Liberty, edite el archivo *<inicio servidor Liberty>*/jvm.options, donde *<inicio servidor Liberty>* es el directorio de inicio del servidor Liberty, por ejemplo /opt/ibm/wlp/usr/servers/defaultServer/jvm.options. Complete uno de los pasos siguientes:
   - Si la autenticación no es necesaria, añada el código siguiente al archivo jvm.options:

     ```
     -Dhttp.proxyHost=<host proxy http>
     -Dhttp.proxyPort=<puerto proxy http>
     -Dhttps.proxyHost=<host proxy https>
     -Dhttps.proxyPort=<puerto proxy https>
     -Djava.net.useSystemProxies=true
     ```

   - Si se necesita un nombre de usuario y una contraseña para acceder al servidor de proxy directo, añada el código siguiente al archivo jvm.options:

     ```
     -Dhttp.proxyHost=<host proxy http>
     -Dhttp.proxyPort=<puerto proxy http>
     -Dhttp.proxyUser=<usuario proxy http>
     -Dhttp.proxyPassword=<contraseña proxy http>
     -Dhttps.proxyHost=<host proxy https>
     -Dhttps.proxyPort=<puerto proxy https>
     -Dhttps.proxyUser=<usuario proxy https>
     -Dhttps.proxyPassword=<contraseña proxy https>
     -Djava.net.useSystemProxies=true
     ```

4. Reinicie la aplicación local para implementar los cambios.

Resultados
Ha configurado los recopiladores de datos para comunicarse a través de un proxy directo.

Nombres de sistema gestionado

El nombre de sistema gestionado (MSN) se utiliza para identificar de forma exclusiva cada agente de Cloud APM dentro del entorno. También es el nombre de instancia que ve en el Panel de instrumentos del rendimiento de aplicaciones cuando selecciona un grupo para cada sistema gestionado desde la sección **Grupos** del navegador. Para evitar conflictos en su entorno, asigne MSN exclusivos a sus agentes.

El formato del MSN del agente difiere en función del tipo de agente. Se encuentra en una de estas categorías:

- "Formato de MSN común para agentes de una sola instancia" en la página 173
- "Formato común de MSN para agentes de varias instancias" en la página 174
- "Formato especial de MSN" en la página 175

Formato de MSN común para agentes de una sola instancia

Para la mayoría de agentes de una sola instancia, el formato común del MSN sigue estas pautas:

```
nombre_host:pc
```

donde:

- *nombre_host* es el nombre del sistema donde se ha instalado el agente. Esta parte se puede cambiar si es necesario.
- *pc* es el código de agente de dos caracteres en mayúsculas y no se puede cambiar. Para obtener más información sobre códigos de agente, consulte "Utilización de mandatos de agente" en la página 184.
- : es el separador y no se puede cambiar.

Ejemplo: `linuxhost01:LZ` es el MSN del Agente de sistema operativo Linux.

Algunos agentes de una sola instancia que no siguen el formato de MSN aparecen en la Tabla 9 en la página 175.

El MSN está limitado a 32 caracteres. Para esta categoría de MSN, hay disponibles 29 caracteres para el nombre de host porque el código de agente y el separador no se pueden cambiar.

Importante: Si la longitud del MSN supera los 32 caracteres, parte del MSN se trunca y no se visualiza correctamente en la Consola de Cloud APM. Por ejemplo, si su nombre de host es `NombreServidorDivisiónVentasMuyLargo03`, el nombre del sistema gestionado debería ser `NombreServidorDivisiónVentasMuyLargo03:PC`. Sin embargo, se trunca en `VeryLongSalesDivisionServerName0`.

Formato común de MSN para agentes de varias instancias

Para agentes de varias instancias, el formato común del MSN sigue estas pautas:

```
nombre_instancia:nombre_host:pc
```

donde:

- *nombre_instancia* es el nombre de instancia de agente que se especifica durante la configuración del agente. Utilice esta variable para garantizar un MSN exclusivo para cada instancia de cada tipo de agente en cada sistema principal de agente.

  Recuerde:

  – Se pueden utilizar letras del alfabeto latino (a-z, A-Z), números arábigos (0-9) y el carácter de guión o signo menos (-) para crear nombres de instancia de agente.
  – El carácter de subrayado (_) no está permitido en los nombres de instancia de agente.
  – El nombre de instancia que especifique está limitado de la manera siguiente:

    - Linux AIX 28 caracteres menos la longitud del nombre de host en sistemas Linux o AIX.
    - Windows 28 caracteres menos la longitud del nombre de host cuando se utiliza el archivo de respuestas silencioso para la configuración en sistemas Windows. Por ejemplo, `Server-Name` tiene 11 caracteres de longitud. Por lo tanto, las instancias de agente en `Server-Name` deben tener como máximo 17 caracteres de longitud.
    - Windows 20 caracteres menos la longitud con la que el nombre de host supera los 8 caracteres cuando se utiliza la configuración de la Consola de Cloud APM en sistemas Windows. Por ejemplo, `TestServer` tiene 10 caracteres, por lo que supera los 8 en 2. Por lo tanto, las instancias de agente en `TestServer` deben tener como máximo 18 caracteres de longitud.
- *nombre_host* es el nombre del sistema donde se ha instalado el agente. El componente de nombre de host del MSN puede cambiarse si es necesario.
- *pc* es el código de agente de dos caracteres en mayúsculas y no se puede cambiar. Para obtener más información sobre códigos de agente, consulte “Utilización de mandatos de agente” en la página 184.
- `:` es el separador y no se puede cambiar.

Ejemplo: `jboss1:win2016:JE` es el MSN del Agente de JBoss.

Algunos agentes de varias instancias que no siguen el formato de MSN aparecen en la Tabla 9 en la página 175.

El MSN está limitado a 32 caracteres. Para esta categoría de MSN, hay disponibles 28 caracteres entre el nombre de la instancia y el nombre de host porque el código de agente y los separadores no se pueden cambiar.

Importante: Si la longitud del MSN supera los 32 caracteres, parte del MSN se trunca y no se visualiza correctamente en la Consola de Cloud APM. Por ejemplo, si especifica `NombreInstanciaMuyLargo` como su nombre de instancia, y el nombre del servidor es `Producción09`, el nombre del sistema

gestionado debería ser NombreInstanciaMuyLargo:Producción09:*PC*. Sin embargo, se trunca en VeryLongInstanceName:Production0.

Formato especial de MSN

Se aplica un formato especial de MSN a los agentes cuyos MSN no sigan las pautas comunes de MSN anteriores. Estos agentes aparecen en la lista de la Tabla 9 en la página 175.

El MSN especia tiene una limitación de 32 caracteres. En la Tabla 9 en la página 175, solamente se pueden cambiar las series en cursiva en la columna de formato de MSN.

Tabla 9. Formato especial de MSN

Agentes	Formato de MSN	Ejemplo de MSN
Agente de Amazon EC2	B5:*nombre_subnodo_ec2*:INS	B5:ventas:INS
Agente de Amazon ELB	• AL:*nombre_instancia*A:APP • AL:*nombre_instancia*C:CLA • AL:*nombre_instancia*N:NET	• AL:elb-inst3A:APP • AL:elb-inst3C:CLA • AL:elb-inst3N:NET
Agente de Azure Compute	AK:*nombre_subnodo_cálculo_azure*:AVM	AK:azc-inst3:AVM
Agente de Citrix VDI	VD:*nombre_sitio_citrix*:XDS	VD:xds1:XDS
Agente de DataPower	BN:*nombre_sistema_datapower*:DPS	BN:datapower23:DPS
Agente de HTTP Server	HU:*alias_nombre_host*:HUS	HU:docker-ihs_httpd:HUS
Agente de IBM Integration Bus	*nomb_interm_superv*:*ID_agente*:KQIB	TRADEBRK:AGT1:KQIB
Agente de MQ Appliance	MK:*nombre_host_nombre_sección*:ARM	MK:bvtmin_linux150:ARM
Agente de Node.js	NJ:*puerto_nombre_host*:NJA	NJ:KVM-014179_3000:NJA
Agente de Oracle Database	• RZ:*conexión_bd-nombre_instancia-nombre_host*:ASM • RZ:*conexión_bd-nombre_instancia-nombre_host*:DG • RZ:*conexión_bd-nombre_instancia-nombre_host*:RDB	RZ:11g-oracledbdemo-GVT-1BL:RDB
Agente de Ruby	KM:*nombre_host-nombre_aplicación*:RAP	KM:nc9098036112_Blog:RAP

Tabla 9. Formato especial de MSN (continuación)

Agentes	Formato de MSN	Ejemplo de MSN
Agente de SAP	• Instancia SAP: *nombre_inst-nombre_host_número_inst_sid*:Ins • SAP Process Integration: *nombre_instancia-nombre_host*:PI • SAP Solution Manager: *nombre_instancia-nombre_host*:Slm • SAP System: *nombre_instancia-nombre_host*:Sys	• PS5-IBMSAP3V1_PS5_11:Ins • PS5-IBMSAP3V1:PI • PS8-IBMSAP3V3:Slm • PS5-IBMSAP3V1:Sys
Agente de SAP HANA Database	• SAP Hana Database: S7:*nombre_bd-ID_sistema*:HDB • SAP Hana System: *nombre_instancia*:*nombre_host*:S7	• S7:HNA-HNA:HDB • HNA:PS8760:S7
Agente de SAP NetWeaver Java Stack	• Clúster SAP NW Java AS: *nombre_instancia*:*nombre_host*:SV • Instancia SAP NW Java AS: SV:*ID_sistema-jvmid*:NWJ	• J01:VPT02F17:SV • SV:J01-83309750:NWJ
Agente de sistema operativo UNIX	*nombre_host*:KUX	worklight17:KUX
Agente de WebLogic	WB:*nombre_instancia*:WLS	WB:Server1:WLS
Agente de WebSphere Applications	• WebSphere Application Server: *alias_servidor*:*nombre_host*:KYNS • WebSphere Portal Server: *alias_servidor*:*nombre_host*:KYNR • WebSphere Process Server: *alias_servidor*:*nombre_host*:KYNP	simpletrade:worklight17:KYNS
Agente de WebSphere MQ	*nom_gestor_colas_superv*:*nom_agente*:MQ	TRADEQM:PoC:MQ
Agente de sistema operativo Windows	Primary:*nombre_host*:NT	Primary:TRADEIIS1:NT

Cambio del nombre del sistema gestionado por el agente

Existen distintos procedimientos para cambiar el nombre de sistema gestionado para los distintos agentes de Cloud APM. Para algunos agentes, cambiar el nombre de sistema gestionado significa cambiar el nombre de host o el nombre de instancia de agente (o ambos) en el nombre de sistema gestionado. Para otros agentes, se requieren procedimientos específicos para cambiar el nombre de sistema gestionado.

Antes de empezar

Familiarícese con los formatos de nombre de sistema gestionado y las restricciones de nomenclatura tal como se describen en "Nombres de sistema gestionado" en la página 173.

Acerca de esta tarea

Para la mayoría de agentes de Cloud APM, puede utilizar el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host utilizado en el nombre de sistema gestionado. Para cambiar el nombre de instancia de agente en el nombre de sistema gestionado para agentes de múltiples instancias, puede utilizar el parámetro de configuración del agente. Si ha configurado el agente, debe volver a configurarlo para asignar un nombre de instancia de agente diferente. Tras volver a configurar el agente, no podrá recuperar los datos recopilados mediante la instancia de agente anterior.

Es posible que no pueda cambiar el nombre de sistema gestionado en un único procedimiento, según qué parte del nombre de sistema gestionado desee cambiar.

Para averiguar el método de cambio de nombre de sistema gestionado para el agente que le interesa, consulte Tabla 10 en la página 177.

Excepción: El cambio de nombre de sistema gestionado no está soportado en Agente de HTTP Server, Agente de Node.js o Agente de Synthetic Playback

Tabla 10. Métodos de cambio de nombre de sistema gestionado para agentes de Cloud APM

Agente	**Método de cambio de nombre de sistema gestionado**
Agente de Amazon EC2	Utilice el parámetro de configuración de agente para cambiar el nombre de subnodo EC2 en el nombre de sistema gestionado, consulte "Parámetros de configuración para el Agente de Amazon EC2" en la página 203.
Agente de Amazon ELB	Cree una nueva instancia de agente con un nuevo nombre de instancia para cambiar el nombre de sistema gestionado.
Agente de Azure Compute	Utilice el parámetro de configuración de agentes para cambiar el nombre de subnodo en el nombre de sistema gestionado. Consulte "Parámetros de configuración para el Agente de Azure Compute" en la página 218.
Agente de Cassandra	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de Cisco UCS	Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia de agente, consulte "Parámetros de configuración del agente" en la página 227.
Agente de Citrix VDI	Utilice el parámetro de configuración de agentes para cambiar el nombre de sitio de Citrix, consulte "Parámetros de configuración para el Agente de Citrix VDI" en la página 237.
Agente de Db2	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.

Tabla 10. Métodos de cambio de nombre de sistema gestionado para agentes de Cloud APM (continuación)

Agente	Método de cambio de nombre de sistema gestionado
Agente de DataPower	Utilice el parámetro de configuración de agentes para cambiar el nombre de sistema gestionado, consulte "Configuración del Agente de DataPower " en la página 248.
Agente de DataStage	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de Hadoop	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.
Agente de HMC Base	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de IBM Cloud	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de IBM Integration Bus	"Especificación de un nombre de sistema gestionado exclusivo para el Agente de IBM Integration Bus" en la página 299
Agente de JBoss	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de Linux KVM	Utilice los parámetros de configuración de agentes, consulte "Configuración de la supervisión de Linux KVM" en la página 490.
Agente de sistema operativo Linux	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.

Tabla 10. Métodos de cambio de nombre de sistema gestionado para agentes de Cloud APM (continuación)

Agente	Método de cambio de nombre de sistema gestionado
Agente de Microsoft .NET	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.
Agente de Microsoft Active Directory	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.
Agente de Microsoft Exchange Server	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.
Agente de Microsoft Hyper-V Server	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.
Agente de Microsoft IIS	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.
Agente de Microsoft Office 365	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.
Agente de Microsoft SQL Server	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de Microsoft SharePoint Server	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.
Agente de MongoDB	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.

Tabla 10. Métodos de cambio de nombre de sistema gestionado para agentes de Cloud APM (continuación)

Agente	Método de cambio de nombre de sistema gestionado
Agente de MySQL	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de NetApp Storage	Utilice los parámetros de configuración de agentes, consulte "Configuración de la supervisión de NetApp Storage" en la página 602.
Agente de OpenStack	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de Oracle Database	Utilice los parámetros de configuración de agentes, consulte "Configuración de la supervisión de base de datos de Oracle" en la página 638.
Agente de PHP	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de PostgreSQL	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de RabbitMQ	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de Supervisión de tiempo de respuesta	"Especificación de un nombre de sistema gestionado exclusivo para el Agente de Supervisión de tiempo de respuesta" en la página 743
Agente de Ruby	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.

Tabla 10. Métodos de cambio de nombre de sistema gestionado para agentes de Cloud APM (continuación)

Agente	Método de cambio de nombre de sistema gestionado
Agente de SAP	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de SAP HANA Database	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de SAP NetWeaver Java Stack	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de Siebel	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de Skype for Business Server (anteriormente conocido como agente de Microsoft Lync Server)	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.
Agente de Sterling File Gateway	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de Sterling Connect Direct	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.

Tabla 10. Métodos de cambio de nombre de sistema gestionado para agentes de Cloud APM (continuación)

Agente	Método de cambio de nombre de sistema gestionado
Agente de Tomcat	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de sistema operativo UNIX	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.
Agente de WebSphere Applications	Para cambiar el nombre de host en el nombre de sistema gestionado, consulte Cómo cambiar el nombre de host utilizado en el nombre de sistema gestionado para la instancia de agente de WAS. Para cambiar el nombre de alias de servidor en el nombre de sistema gestionado, vuelva a configurar el agente. Consulte "Reconfiguración interactiva del recopilador de datos" en la página 875.
Agente de WebSphere Infrastructure Manager	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182. Utilice el parámetro de configuración de agentes para cambiar el nombre de instancia en el nombre de sistema gestionado.
Agente de WebSphere MQ	"Especificación de nombres de sistema gestionado exclusivos para varios gestores de colas" en la página 971
Agente de sistema operativo Windows	Utilice el parámetro **CTIRA_HOSTNAME** para cambiar el nombre de host en el nombre de sistema gestionado. Consulte "Cambio del nombre de host en el nombre de sistema gestionado" en la página 182.

Cambio del nombre de host en el nombre de sistema gestionado

Acerca de esta tarea

No es una práctica común cambiar el nombre de host en el nombre de sistema gestionado. El nombre de host se detecta y establece automáticamente durante la configuración del agente. Cambie el nombre de host en el nombre de sistema gestionado sólo cuando sea necesario y asegúrese de que el valor que especifica no causa truncamientos debido a restricciones de nomenclatura del nombre del sistema gestionado.

Procedimiento

1. Detenga todas las instancias existentes del agente y espere a que la Consola de Cloud APM muestre que el agente o sus subnodos está fuera de línea. Si no tiene ninguna instancias de agente existente, continúe con el paso siguiente.

   Para obtener más información sobre cómo detener instancias de agente, consulte "Utilización de mandatos de agente" en la página 184.

2. Si el agente es un agente de una sola instancia, siga estos pasos para cambiar el parámetro **CTIRA_HOSTNAME**. El valor que especifique para el parámetro **CTIRA_HOSTNAME** es el valor que se aplica a todas las instancias del agente nuevo.
   a) Realice una copia de seguridad del archivo siguiente:
      - Linux AIX *dir_instalación*/config/*cp*.environment
      - Windows *dir_instalación*\TMAITM6_x64\k*pc*cma.ini

      donde:
      - *dir_instalación* es el directorio de instalación del agente.
      - *pc* es el código de agente de dos caracteres. Consulte la Tabla de nombres de agente y códigos de agente.
   b) Edite el archivo cambiando el valor del parámetro **CTIRA_HOSTNAME** tal como se indica a continuación, donde *nombre_host_nuevo* es la serie personalizada que se utiliza en lugar del nombre de host real del equipo donde se ha instalado el agente.
      - Linux AIX **CTIRA_HOSTNAME**=*nuevo_nombre_host*
      - Windows **CTIRA_HOSTNAME**=*nombre_host_nuevo* .TYPE=REG_EXPAND_SZ
   c) Guarde los cambios.
3. Si el agente es un agente de varias instancias, siga estos pasos para cambiar el parámetro **CTIRA_HOSTNAME**. Normalmente, todas las instancias de agente de un sistema utilizan el mismo valor de nombre de host. Si necesita que las instancias de agente utilicen valores diferentes, varíe el valor asignado a **CTIRA_HOSTNAME** al ejecutar este paso.
   a) Realice una copia de seguridad de los archivos siguientes:
      - Linux AIX *dir_instalación*/config/*pc_instancia*.environment
      - Windows *dir_instalación*\TMAITM6_x64\k*pc*cma_*instancia*.ini
   b) Edite el archivo y cambie el valor del parámetro **CTIRA_HOSTNAME** tal como se indica a continuación:
      - Linux AIX **CTIRA_HOSTNAME**=*nuevo_nombre_host*
      - Windows **CTIRA_HOSTNAME**=*nombre_host_nuevo* .TYPE=REG_EXPAND_SZ
   c) Guarde los cambios.
4. Windows
   Reconfigure las instancias de agente existentes.
5. Inicie todas las instancias de agente.

Qué hacer a continuación

Cuando haya cambiado el nombre de sistema gestionado del agente, inicie la Consola de Cloud APM y modifique sus aplicaciones eliminando el nombre de sistema gestionado anterior de las aplicaciones y añadiendo el nuevo nombre de sistema gestionado en su lugar.

Configuración de agentes

Después de la instalación, algunos agentes se configuran e inician automáticamente, mientras que otros requieren configuración manual pero se inician automáticamente. Algunos agentes se deben configurar e iniciar manualmente. Los agentes de varias instancias requieren que se cree una primera instancia y se inicie de forma manual.

Antes de empezar

Cuando instala un agente, se coloca un archivo de configuración silenciosa de muestra en el directorio `/opt/ibm/apm/agent/samples`, por ejemplo `ynv_silent_config_agent.txt` y `datapower_silent_config.txt`.

Nota: Algunos agentes, por ejemplo Monitoring Agent for WebSphere Applications, tienen varios archivos de configuración silenciosa para diferentes tareas, como por ejemplo la configuración del recopilador de datos.

Acerca de esta tarea
Para obtener información de despliegue específica para los agentes, consulte Capítulo 5, “Despliegue de agentes y recopiladores de datos”, en la página 117.

Para configurar un agente, puede utilizar la línea de mandatos o un archivo de respuestas silencioso, tal como se describe en este procedimiento.

Los métodos de configuración varían según los agentes; utilice el procedimiento proporcionado para su agente.

Procedimiento

- Ejecute el mandato *nombre_agente*`.sh config .`
  Para ver más mandatos, consulte la Tabla 12 en la página 187 y la Tabla 13 en la página 188.
- Edite el archivo de respuestas silencioso y, a continuación, ejecute uno de los mandatos siguientes:
  - Para agentes de instancia única, ejecute el mandato siguiente:

    ```
    nombre_agente.sh config archivo_respuestas
    ```

  - Para agentes de varias instancias, ejecute el mandato siguiente:

    ```
    nombre_agente.sh config nombre_instancia archivo_respuestas
    ```

  - donde *nombre_instancia* es el nombre de instancia que se puede asignar para indicar lo que está supervisando.
- Windows
  Para los agentes soportados en sistemas Windows, puede realizar determinadas tareas de configuración mediante la ventanaIBM Cloud Application Performance Management. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.Para obtener más información, consulte “Utilización de la ventana de IBM Cloud Application Performance Management en sistemas Windows” en la página 189.
- Para realizar la configuración avanzada de determinados agentes como, por ejemplo, configurar el rastreo de transacciones o la recopilación de datos, y habilitar datos de diagnóstico, utilice la ventana **Configuración del agente**. Para obtener más información, consulte “Página Configuración de agente” en la página 189.

Utilización de mandatos de agente
Los mismos scripts que utiliza para instalar agentes de supervisión también se utilizan para comprobar el estado de un agente instalado, detenerlo o iniciarlo, o desinstalar el agente.

Acerca de esta tarea
El nombre del agente y los códigos de agente se proporcionan a modo de referencia.

Utilice el nombre de agente en los mandatos siguientes:

Linux AIX *nombre*`-agent.sh`
Windows *nombre*`-agent.bat`

Donde *nombre* es el nombre del agente que se ha especificado en Tabla 11 en la página 185.

Tabla 11. Nombres de agente y códigos de agente

Agente de supervisión	***nombre***	**Código de dos letras del agente**
Monitoring Agent for Amazon EC2	`amazon_ec2`	`b5`
Monitoring Agent for Azure Compute	`azure_compute`	`ak`
Monitoring Agent for Cassandra	`cassandra`	`zc`
Monitoring Agent for Cisco UCS	`cisco_ucs`	`v6`
Monitoring Agent for Citrix Virtual Desktop Infrastructure	`citrix_vdi`	`vd`
Monitoring Agent for DataPower	`datapower`	`bn`
Monitoring Agent for Db2	`db2`	`ud`
Monitoring Agent for Hadoop	`hadoop`	`h8`
Monitoring Agent for HMC Base	`hmc_base`	`ph`
Monitoring Agent for HTTP Server	`servidor_http`	`hu`
Monitoring Agent for IBM Cloud	`ibm_cloud`	`fs`
Monitoring Agent for IBM Integration Bus	`iib`	`qi`
Monitoring Agent for MQ Appliance	`ibm_mq_appliances`	`mk`
Monitoring Agent for InfoSphere DataStage	`datastage`	`dt`
Monitoring Agent for JBoss	`jboss`	`je`
Monitoring Agent for Linux KVM	`linux_kvm`	`v1`
Monitoring Agent for Linux OS	`os`	`lz`
Monitoring Agent for MariaDB	`mariadb`	`mj`
Monitoring Agent for Microsoft Active Directory	`msad`	`3z`
Monitoring Agent for Microsoft Cluster Server	`mscs`	`q5`
Monitoring Agent for Microsoft Exchange Server	`msexch`	`ex`
Monitoring Agent for Microsoft Hyper-V Server	`microsoft_hyper-v_server`	`hv`
Monitoring Agent for Microsoft Internet Information Services	`msiis`	`q7`
Monitoring Agent for Skype for Business Server (anteriormente conocido como Microsoft Lync Server)	`skype_for_business_server`	`ql`
Monitoring Agent for Microsoft .NET	`dotnet`	`qe`
Monitoring Agent for Microsoft Office 365	`microsoft_office365`	`mo`
Monitoring Agent for Microsoft SharePoint Server	`ms_sharepoint_server`	`qp`
Monitoring Agent for Microsoft SQL Server	`mssql`	`oq`
Monitoring Agent for MongoDB	`mongodb`	`kj`
Monitoring Agent for MySQL	`mysql`	`se`

Tabla 11. Nombres de agente y códigos de agente (continuación)		
Agente de supervisión	***nombre***	**Código de dos letras del agente**
Monitoring Agent for NetApp Storage	`netapp_storage`	`nu`
Monitoring Agent for Node.js	`nodejs`	`nj`
Monitoring Agent for OpenStack	`openstack`	`sg`
Monitoring Agent for Oracle Database	`oracle_database`	`rz`
Monitoring Agent for PHP	`php`	`pj`
Monitoring Agent for PostgreSQL	`postgresql`	`pn`
Monitoring Agent for Python	`python`	`pg`
Monitoring Agent for RabbitMQ	`rabbitMQ`	`zr`
Monitoring Agent for Ruby	`ruby`	`km`
Monitoring Agent for SAP Applications	`sap`	`sa`
Monitoring Agent for SAP HANA Database	`sap_hana_database`	`s7`
Monitoring Agent for SAP NetWeaver Java Stack	`sap_netweaver_java_stack`	`sv`
Monitoring Agent for Siebel	`siebel`	`uy`
Monitoring Agent for Sterling Connect Direct	`sterling_connect_direct-agent`	`FC`
Monitoring Agent for Sterling File Gateway	file_gateway	`fg`
Monitoring Agent for Sybase Server	sybase	`oy`
Monitoring Agent for Synthetic Playback	`synthetic_transactions`	`sn`
Monitoring Agent for Tomcat	`tomcat`	`ot`
Monitoring Agent for UNIX OS	`os`	`ux`
Monitoring Agent for VMware VI	`vmware_vi`	`vm`
Monitoring Agent for WebLogic	`oracle_weblogic`	`wb`
Monitoring Agent for WebSphere Applications	`was`	`yn`
Monitoring Agent for WebSphere Infrastructure Manager	`wim`	`d0`
Monitoring Agent for WebSphere MQ	`mq`	`mq`
Monitoring Agent for Windows OS	`os`	`nt`
Agente de Supervisión de tiempo de respuesta	`rt`	`t5`

Procedimiento

- Linux AIX
  En el sistema en donde desee enviar un mandato al agente de supervisión, vaya al directorio *`dir_instalación`*`/bin`. Especifique cualquiera de los mandatos en Tabla 12 en la página 187 donde *nombre* es el nombre de agente que se especifica en Tabla 11 en la página 185.

Tabla 12. Mandatos para sistemas UNIX y Linux	
Mandato	**Descripción**
./*nombre*-agent.sh status	Comprueba el estado del agente. El estado puede ser en ejecución o no en ejecución. Cuando el agente está en ejecución, el estado de conexión entre el agente y el Servidor de Cloud APM también está seleccionado. Los posibles estados negativos de conexión son: Error de conexión, Error detectado, Error-Desconectado. El estado positivo es Conectado, este es el estado esperado. El estado de transición es Conectando. El estado Desconocido significa que el estado del agente no se puede reconocer, es posible que sea debido a errores en el sistema de archivos o en el archivo de registro del agente.
./*nombre*-agent.sh start	Inicia el agente de supervisión. Si el agente tiene instancias, especifique un nombre de instancia después del mandato.
./*nombre*-agent.sh stop	Detiene el agente. Si el agente tiene instancias, especifique un nombre de instancia después del mandato.
./*nombre*-agent.sh prereqcheck	Ejecuta una exploración de requisitos previos. Esta opción de mandato está disponible para la mayoría de agentes.
./*nombre*-agent.sh install	Instala el agente de supervisión. Si desea más información, consulte "Instalación de agentes en sistemas UNIX" en la página 126 y "Instalación de agentes en sistemas Linux" en la página 132.
./*nombre*-agent.sh config *nombre_instancia vía_acceso_a_archivo_config_silencioso*	Configura el agente de supervisión. Ejecute el mandato desde el directorio *dir_instalación*/bin y añada la vía de acceso del archivo de respuestas si es necesario. Si el agente tiene instancias, especifique un nombre de instancia. Para obtener más información sobre qué agentes son agentes de varias instancias, consulte Tabla 7 en la página 119 . El *archivo_config_silencioso* es opcional. Si no especifica un archivo para la configuración silenciosa, puede configurar el agente de supervisión interactivamente siguiendo las solicitudes.
./*nombre*-agent.sh uninstall	Desinstala el agente de supervisión. Para obtener más información, consulte "Desinstalación de los agentes" en la página 151.
./smai-agent.sh uninstall_all	Desinstala todos los agentes de supervisión en el sistema gestionado.
./*nombre*-agent.sh remove *nombre_instancia*	Elimina una instancia de un agente de varias instancias.

Tabla 12. Mandatos para sistemas UNIX y Linux (continuación)	
Mandato	**Descripción**
`./`*nombre*`-agent.sh`	Ver una descripción de las funciones disponibles con el script.

- Windows

En el sistema en donde desee enviar un mandato al agente de supervisión, vaya al directorio *dir_instalación*`\BIN` en el indicador de mandatos, por ejemplo: `C:\IBM\APM\bin`. Especifique cualquiera de los mandatos en Tabla 13 en la página 188 donde *nombre* es el nombre de agente que se especifica en Tabla 11 en la página 185.

Tabla 13. Mandatos para sistemas Windows	
Mandato	**Descripción**
nombre`-agent.bat status`	Comprueba el estado del agente. Comprueba el estado de la conexión entre el agente y el Servidor de Cloud APM. Los posibles estados negativos de conexión son: Error de conexión, Error detectado, Error-Desconectado. El estado positivo es Conectado, este es el estado esperado. El estado de transición es Conectando. El estado Desconocido significa que el estado del agente no se puede reconocer, es posible que sea debido a errores en el sistema de archivos o en el archivo de registro del agente.
nombre`-agent.bat start`	Inicia el agente de supervisión. Si el agente tiene instancias, especifique un nombre de instancia después del mandato.
nombre`-agent.bat stop`	Detiene el agente. Si el agente tiene instancias, especifique un nombre de instancia después del mandato.
nombre`-agent.bat prereqcheck`	Ejecuta una exploración de requisitos previos. Esta opción de mandato está disponible para la mayoría de agentes.
nombre`-agent.bat install`	Instala el agente de supervisión. Para obtener más información, consulte "Instalación de agentes" en la página 144.
nombre`-agent.bat config` *nombre_instancia vía_acceso_a_archivo_configuración_silenciosa*	Configura el agente de supervisión. Ejecute el mandato desde el directorio *dir_instalación*`\bin` y añada la vía de acceso del archivo de respuestas si es necesario. Si el agente tiene instancias, especifique un nombre de instancia. Para obtener más información sobre qué agentes son agentes de varias instancias, consulte Tabla 7 en la página 119 . El *archivo_config_silencioso* es opcional. Si no especifica un archivo para la configuración silenciosa, puede configurar el agente de supervisión interactivamente siguiendo las solicitudes.

Tabla 13. Mandatos para sistemas Windows (continuación)	
Mandato	**Descripción**
nombre-agent.bat uninstall	Desinstala el agente de supervisión. Para obtener más información, consulte "Desinstalación de los agentes" en la página 151.
smai-agent.bat uninstall_all	Desinstala todos los agentes de supervisión en el sistema gestionado.
nombre-agent.bat remove *nombre_instancia*	Elimina una instancia de un agente de varias instancias.
nombre-agent.bat	Ver una descripción de las funciones disponibles con el script.

Mandato de versión de agente

- Para ver la versión del agente en el entorno, ejecute los siguientes mandatos:
  - Linux AIX

    ```
    dir_instalación/bin/cinfo
    ```

    Especifique 1 para mostrar las versiones.
  - Windows

    ```
    dir_instalación/InstallITM/kincinfo
    ```

Tareas relacionadas

"Utilización de la ventana de IBM Cloud Application Performance Management en sistemas Windows" en la página 189

Utilización de la ventana de IBM Cloud Application Performance Management en sistemas Windows

Los agentes soportados de Windows tienen un programa de utilidad de interfaz gráfica de usuario que puede utilizar para realizar la configuración del agente y comprobar el estado de conexión.

El programa de utilidad de configuración de la interfaz gráfica de usuario no está disponible para el Monitoring Agent for WebSphere MQ o el Monitoring Agent for IBM Integration Bus.

Procedimiento

- Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.

Resultados

Aparece la ventana de IBM Cloud Application Performance Management. Cada componente de agente instalado se lista con su estado de configuración, si está iniciado o detenido, el estado de conexión, el número de versión, y otra información.

Qué hacer a continuación

Inicie o detenga un agente o configure los parámetros pulsando con el botón derecho sobre el agente y seleccionando una opción.

Página Configuración de agente

Utilice la página **Configuración de agente** para configurar centralmente los valores para agentes como Agente de Supervisión de tiempo de respuesta y Agente de WebSphere Applications.

Uso general

Después de pulsar **Configuración del sistema** > **Configuración de agente** desde la barra de navegación, se muestra un panel instrumentos con pestañas con una pestaña para cada agente de supervisión configurable. La tabla muestra columnas de información de configuración, como el nombre y la dirección IP y una fila para cada sistema gestionado.

Acciones

Utilice las opciones de Acciones para habilitar o inhabilitar funciones como el rastreo de transacciones o la recopilación de datos.

Redimensionamiento de columna

Arrastre un marco de cabecera de columna para ajustar el ancho de columna.

Clasificación de columnas

Pulse dentro de una cabecera de columna para clasificar esa columna. Vuelva a pulsar la misma cabecera de columna para cambiar entre orden de clasificación ascendente y descendente.

Filtro de tabla

Pulse dentro del recuadro de texto de filtro  y escriba el principio del valor por el que va filtrar la tabla. A medida que escribe, las filas de la tabla que no coincidan con los criterios se filtrarán y se actualizará el ***Total*** para el número de filas encontrado.

Pulse la "x" en el recuadro de filtro  o pulse la tecla de retroceso para borrar el filtro.

Configuración del agente

Para obtener más información sobre los valores de los agentes específicos, consulte los temas siguientes:

- Agente de DataPower : “Configuración de la supervisión DataPower” en la página 240
- Agente de IBM Integration Bus: “Configuración del rastreo de transacciones para el Agente de IBM Integration Bus” en la página 299
- Internet Service Monitoring“Configuración del agente en sistemas Windows ” en la página 464
- Agente de JBoss: “Configurar el recopilador de datos de rastreo de transacciones del Agente de JBoss” en la página 486
- Agente de Microsoft .NET: “Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones” en la página 545
- Supervisión de archivo de registro de agente de sistema operativo: “Adición o eliminación de la configuración de supervisión de archivos de registro para los agentes de sistema operativo” en la página 656
- Agente de Supervisión de tiempo de respuesta: “Configuración de la página Configuración de agente” en la página 717
- Geolocalización: “Personalización de valores de ubicación de transacciones de usuario final” en la página 738
- Agente de Ruby: “Inhabilitación o habilitación de datos de diagnóstico para aplicaciones Ruby” en la página 751
- Agente de SAP NetWeaver Java Stack: “Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones” en la página 797
- Agente de Tomcat: “Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones” en la página 835
- Agente de WebLogic: “Configuración del rastreo de transacciones para el Agente de WebLogic” en la página 855
- Agente de WebSphere Applications: “Configuración dinámica de la recopilación de datos en la página Configuración de agente” en la página 907
- Agente de WebSphere MQ: “Configuración del rastreo de transacciones para el Agente de WebSphere MQ” en la página 973

Configuración de agentes como usuarios no root

Si desea configurar el agente como un usuario no root, cree un grupo común en el sistema y convierta a cada usuario en un miembro de este grupo.

Antes de empezar

Si ha instalado el agente mediante un usuario root o no root y desea configurar el agente mediante el mismo usuario, no se necesita ninguna acción especial.

Si ha instalado el agente mediante un usuario seleccionado y desea configurar el agente mediante un usuario distinto, cree un grupo común en el sistema. Haga a todos los miembros usuarios de gestión de agentes de este grupo común. Transfiera la transferencia de todos los archivos de agente y directorios a este grupo.

Nota:

- Para el Agente de HTTP Server, si configura el agente como usuario no root, este último debe tener el mismo ID de usuario que el que ha iniciado el IBM HTTP Server. De lo contrario, el agente tendrá problemas para descubrir el IBM HTTP Server.
- Para el Agente de IBM Integration Bus, si la instalación de IBM Integration Bus es un despliegue de un solo usuario, utilice el mismo ID de usuario con el que ha instalado IBM Integration Bus para configurar el agente. Antes de configurar el agente, realice los pasos siguientes para este ID de usuario.

Procedimiento

1. Instale los agentes de supervisión en Linux o UNIX tal como se describe en "Instalación de agentes en sistemas Linux" en la página 132 y "Instalación de agentes en sistemas UNIX" en la página 126.
2. Ejecute el script `./secure.sh` con el nombre de grupo del usuario no root para proteger los archivos y establecer la propiedad del grupo de archivos en los archivos.
   Por ejemplo: **`./secure.sh -g db2iadm1`**
3. Configure los agentes de supervisión en Linux o AIX como corresponda, consulte Capítulo 7, "Configuración del entorno", en la página 165.
4. Para actualizar los scripts de arranque del sistema, ejecute el script siguiente con el usuario rooto sudo: *dir_instalación*`/bin/UpdateAutoRun.sh`

Qué hacer a continuación

Para obtener más información sobre el script **`./secure.sh`**, consulte Asegurar los archivos de instalación de agente.

Utilice el mismo ID de usuario para la instalación del agente y para las actualizaciones.

Inhabilitación del inicio automático de agente en sistemas UNIX y Linux

En un sistema UNIX o Linux, se puede iniciar automáticamente un agente después de un reinicio del sistema operativo. Si no desea que el agente se inicie automáticamente después de reiniciar el sistema, puede inhabilitar el inicio automático de agente.

Acerca de esta tarea

Si instala un agente como usuario root en el sistema UNIX o Linux, se puede iniciar automáticamente el agente después de reiniciar el sistema. Si instala un agente como usuario no root pero ejecuta el script **`UpdateAutoRun.sh`** como root después de la instalación, se puede iniciar automáticamente el agente después de reiniciar el sistema.

Procedimiento

1. Realice los siguientes pasos para inhabilitar el inicio automático en algunos agentes:

a. Para el agente de aplicaciones de Agente de sistema operativo Linux y WebSphere®, añada el siguiente código al archivo `agent_install_dir/registry/kcirunas.cfg`:

```
<productCode>lz</productCode>
 <default>
   <autoStart>no</autoStart>
 </default>
 <productCode>yn</productCode>
 <default>
   <autoStart>no</autoStart>
 </default>
```

b. Ejecute el mandato **dir_instalación_agente/bin/UpdateAutoRun.sh**.

2. Realice los siguientes pasos para habilitar el inicio automático en algunos agentes:

a. Para el Agente de sistema operativo Linux y el agente de WebSphere® Applications, en el archivo `dir_instalación_agente/registry/kcirunas.cfg`, cambie el valor de la etiqueta *<autoStart>* a **yes**.

b. Abra el archivo `dir_instalación_agente/registry/AutoStart` y compruebe el contenido.

c. Suprima el archivo `/etc/init.d/ITMAgents{$Num}`, donde *{$Num}* es un número positivo en el archivo `dir_instalación_agente/registry/AutoStart`. Si el valor es 1, debe suprimir el archivo `/etc/init.d/ITMAgents1`.

d. Ejecute el mandato **dir_instalación_agente/bin/UpdateAutoRun.sh**.

Resultados

Después de reiniciar el sistema, un script de agente no se ejecutará automáticamente para iniciar el agente.

Procedimiento general para configurar recopiladores de datos

Para utilizar un recopilador de datos para ver los datos de supervisión en la Consola de Cloud APM para las aplicaciones, debe completar varias tareas de configuración.

Acerca de esta tarea

Este procedimiento es una hoja de ruta para configurar la supervisión de las aplicaciones e incluye pasos necesarios, condicionales y opcionales. Siga los pasos necesarios según sus necesidades.

Procedimiento

1. Descargue y extraiga el paquete del recopilador de datos. Para obtener instrucciones, consulte "Descarga de los agentes y recopiladores de datos" en la página 107.
2. Configure el recopilador de datos para recopilar datos de supervisión acerca de las aplicaciones de IBM Cloud y locales y enviarlos al Servidor de Cloud APM. Realice una o varias de las tareas siguientes según el tipo de la aplicación:

Aplicaciones Liberty

- "Configuración del recopilador de datos para aplicaciones locales" en la página 912
- "Configuración del recopilador de datos de Liberty para aplicaciones IBM Cloud" en la página 916

Aplicaciones Node.js

- "Configuración del Recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud (anteriormente Bluemix)" en la página 615
- "Configuración del Recopilador de datos de Node.js autónomo para aplicaciones locales" en la página 621

Aplicaciones Python

- "Configuración del recopilador de datos de Python para aplicaciones IBM Cloud" en la página 695
- "Configuración del Recopilador de datos de Python para aplicaciones locales" en la página 701

Aplicaciones Ruby

- "Configuración del Recopilador de datos de Ruby para aplicaciones de IBM Cloud" en la página 751

Aplicaciones Java

- "Configuración de la supervisión de J2SE" en la página 468

3. Si el archivo de claves o el Servidor de Cloud APM cambian, vuelva a conectar el recopilador de datos al Servidor de Cloud APM. Para obtener instrucciones, consulte "Reconexión del recopilador de datos al Servidor de Cloud APM" en la página 193.

Qué hacer a continuación

Después de completar todas las tareas de configuración necesarias, puede verificar que los datos de supervisión de la aplicación IBM Cloud se visualizan en la consola de Cloud APM.

Reconexión del recopilador de datos al Servidor de Cloud APM
Si el Servidor de Cloud APM, el archivo de claves o la contraseña del archivo de claves cambian, debe establecer varias variables de entorno para volver a conectar el recopilador de datos al Servidor de Cloud APM.

Antes de empezar
Si el archivo de claves ha cambiado, cifre primero la contraseña de texto sin formato del archivo de claves utilizando Base64. Si es usuario de Linux, ejecute el mandato siguiente:

```
echo -n contraseña_archivo_claves | base64
```

La salida del mandato es la contraseña cifrada. Por ejemplo, si la contraseña de texto sin formato es `password`, la salida del mandato `cGFzc3dvcmQ=` es la contraseña cifrada. A continuación, puede utilizar la contraseña cifrada para establecer `APM_KEYFILE_PSWD:` *`contraseña_archivo_claves_cifrada`* y `APM_KEYFILE_PSWD=`*`contraseña_archivo_claves_cifrada`* en las siguientes configuraciones.

Procedimiento

- Para reconectar los recopiladores de datos al Servidor de Cloud APM para aplicaciones IBM Cloud, consulte "Reconexión de los recopiladores de datos para aplicaciones IBM Cloud" en la página 193.
- Para reconectar los recopiladores de datos al Servidor de Cloud APM para aplicaciones locales, consulte "Reconexión del recopilador de datos para aplicaciones locales" en la página 194.

Reconexión de los recopiladores de datos para aplicaciones IBM Cloud

Acerca de esta tarea

Tiene las dos opciones siguientes para conectar el recopilador de datos al Servidor de Cloud APM:

- Edite el archivo `manifest.yml` de la aplicación para establecer las variables.
- Establezca las variables en la interfaz de usuario de IBM Cloud.

Procedimiento

- Para utilizar el archivo `manifest.yml` de la aplicación IBM Cloud para volver a conectar el recopilador de datos, realice los pasos siguientes:

a) Edite las variables del archivo `manifest.yml` de la aplicación IBM Cloud de acuerdo con los cambios.

   – Para configurar la pasarela para utilizar *HTTP*, establezca la variable siguiente:

   ```
   APM_BM_GATEWAY_URL: http://ip_o_nombre_host_servidor:80
   ```

   – Para configurar la pasarela para utilizar *HTTPS*, establezca las tres variables siguientes:

   ```
   APM_BM_GATEWAY_URL: https://ip_o_nombre_host_servidor:443
   APM_KEYFILE_PSWD: contraseña_archivo_claves_cifrada
   APM_KEYFILE_URL: http://servidor_http_alojado:puerto/nombre_archivo_claves
   ```

   Consejo: El archivo de claves del recopilador de datos Liberty es un archivo `.jks`. Para los recopiladores de datos Python, Node.js y Liberty, los archivos de claves son archivos `.p12`.

b) Vaya al directorio de la aplicación IBM Cloud y ejecute el mandato siguiente:

   ```
   cf push
   ```

- Para utilizar la interfaz de usuario de IBM Cloud para reconectar el recopilador de datos, siga estos pasos:

  a) Inicie sesión en la interfaz de usuario de IBM Cloud.

  b) Pulse la aplicación IBM Cloud.

  c) Pulse **Tiempo de ejecución** en el panel izquierdo.

  d) Vaya a la pestaña **Variable de entorno**.

  e) En la sección **definida por el usuario**, utilice uno de los métodos siguientes para definir las variables según sus necesidades:

  – Para configurar la pasarela para utilizar *HTTP*, establezca la variable siguiente:

  ```
  APM_BM_GATEWAY_URL: http://ip_o_nombre_host_servidor:80
  ```

  – Para configurar la pasarela para utilizar *HTTPS*, establezca las tres variables siguientes:

  ```
  APM_BM_GATEWAY_URL: https://ip_o_nombre_host_servidor:443
  APM_KEYFILE_PSWD: contraseña_archivo_claves_cifrada
  APM_KEYFILE_URL: http://servidor_http_alojado:puerto/nombre_archivo_claves
  ```

  Consejo: El archivo de claves del recopilador de datos Liberty es un archivo `.jks`. Para los recopiladores de datos Python, Node.js y Liberty, los archivos de claves son archivos `.p12`.

  f) Desde el directorio donde ha ejecutado el mandato **`cf push`** para enviar la aplicación, ejecute el mandato siguiente para que los cambios entren en vigor:

  ```
  cf restage <nombre_aplicación>
  ```

Resultados

Los valores de las variables se han establecido adecuadamente para conectar el recopilador de datos al Servidor de Cloud APM.

Reconexión del recopilador de datos para aplicaciones locales

Acerca de esta tarea

Modificando el archivo `global.environment` o `dc.java.properties`, puede personalizar la conexión entre el recopilador de datos y el servidor de Cloud APM.

Procedimiento

1. Busque el archivo correspondiente que contiene las variables de conexión.
   a) Para el Recopilador de datos de Liberty, el Recopilador de datos de Node.js y el Recopilador de datos de Python, busque el archivo `global.environment` de acuerdo con la información de la tabla siguiente:

Nombre de recopilador de datos	Directorio al archivo `global.environment`
Recopilador de datos de Liberty	La carpeta `itcamdc/etc/global.environment` donde está instalado el Recopilador de datos de Liberty.
Recopilador de datos de Node.js	La carpeta `ibmapm/etc` donde está instalado el Recopilador de datos de Node.js.
Recopilador de datos de Python	La carpeta `etc` donde está instalado el Recopilador de datos de Python.

   b) Para el Recopilador de datos de J2SE, busque el archivo `dc.java.properties` en la carpeta *DC_HOME*`/itcamdc/etc`. *DC_HOME* es el directorio donde está instalado el Recopilador de datos de J2SE.
2. Edite las variables del archivo correspondiente de acuerdo con los cambios.
   a) Para el Recopilador de datos de Liberty, el Recopilador de datos de Node.js y el Recopilador de datos de Python, edite el archivo `global.environment` de acuerdo con las instrucciones siguientes:
      - Para configurar la pasarela para utilizar *HTTP*, establezca la variable siguiente:

```
APM_BM_GATEWAY_URL=http://ip_o_nombrehost_servidor:80
```

      - Para configurar la pasarela para utilizar *HTTPS*, establezca las variables siguientes:

```
APM_BM_GATEWAY_URL=https://ip_o_nombrehost_servidor:443
APM_KEYFILE_PSWD=contraseña_archivo_claves_cifrada
APM_KEYFILE_URL= http://servidor_http_alojado:puerto/nombre_archivo_claves
```

      Consejo: El archivo de claves para el Recopilador de datos de Liberty es un archivo `.jks`. Para los recopiladores de datos Python, Node.js y Liberty, los archivos de claves son archivos `.p12`.
   b) Para el Recopilador de datos de J2SE, edite el archivo `dc.java.properties` según las instrucciones siguientes:
      - Para configurar la pasarela para utilizar *HTTP*, establezca la variable siguiente:

```
apm.http.type=http
```

        Si el valor de esta variable se deja vacío, `http` es el valor predeterminado
      - Para configurar la pasarela para utilizar *HTTPS*, establezca las variables siguientes:

```
apm.ssl.password=contraseña_archivo_claves_cifrada
apm.http.type=https
```

      Importante: Si se cambia la contraseña, sustituya el archivo *DC_HOME*`/itcamdc/etc/keyfile.jks` por el archivo `/opt/ibm/ccm/keyfiles/default.agent/keyfiles/keyfile.jks` del servidor de APM Cloud, donde *DC_HOME* es el directorio de inicio del Recopilador de datos de J2SE.
3. Opcional: Si no utiliza el archivo de claves predeterminado para el Recopilador de datos de Node.js, establezca la variable siguiente:

```
APM_SNI=owner_host_en_el_archivo_claves
```

Consejo: Para averiguar el valor de la variable *owner host*, abra el archivo de claves que utilice y busque `owner`. A continuación, establezca la variable *APM_SNI* en el mismo valor de *owner*.

4. Reinicie la aplicación para que el cambio entre en vigor.

Resultados
Los valores de las variables se han establecido adecuadamente para conectar el recopilador de datos al Servidor de Cloud APM.

Ejemplo de archivo `manifest.yml`
Consulte las líneas siguientes para conocer el contenido del archivo `manifest.yml` de una aplicación IBM Cloud:

```
applications:

- disk_quota: 1024M
  host: myBluemixApp
  name: myBluemixApp
  path: .
  domain: mybluemix.net

  instances: 1
  memory: 512M

  env:    KNJ_ENABLE_TT: "true"
    KNJ_SAMPLING: 1
```

Eliminación de recopiladores de datos de Consola de Cloud APM
Tras desconfigurar un recopilador de datos, debe eliminar también el recopilador de datos de las aplicaciones y de los grupos de recursos a los que se había añadido. De lo contrario, la Consola de Cloud APM mostrará que no hay datos disponibles para la aplicación y no indicará que el recopilador de datos está fuera de línea.

Procedimiento

1. Elimine el recopilador de datos de las aplicaciones a las que lo haya añadido editando manualmente las aplicaciones.

   Es parecido a eliminar los agentes fuera de línea de la aplicación. Consulte "Visualización y eliminación de agentes fuera de línea" en la página 1138.
2. Elimine el recopilador de datos de los grupos de recursos personalizados a los que lo haya añadido.

   Para obtener más información, consulte "Gestor de grupos de recursos" en la página 1014.
3. Abra un tíquet para que el equipo de Cloud APM Operations realice los pasos siguientes en el Servidor de Cloud APM:
   a) Edite el archivo *dir_instalación*`/serveragents/config/hostname_bi.cfg` para eliminar las líneas del recopilador de datos que se ha desconfigurado.
   b) Reinicie el componente de servidor para los recopiladores de datos ejecutando el mandato siguiente como usuario root:

      ```
      apm restart biagent
      ```

Resultados

Tras algunos minutos, la Consola de Cloud APM indicará que el recopilador de datos está fuera de línea en la aplicación **Mis componentes** y en la interfaz de usuario **Gestor de grupos de recursos** cuando seleccione el grupo de recursos del sistema para el recopilador de datos.

Tras el intervalo especificado por la propiedad de configuración **Eliminar retardo de sistema fuera de línea** en la página **Configuración avanzada**, el recopilador de datos se eliminará automáticamente de **Mis componentes** y de su grupos de recursos del sistema.

Consejo: Puede ajustar el valor **Eliminar retardo de sistema fuera de línea** en la página **Configuración avanzada** para incrementar o reducir el tiempo de espera antes de que el agente fuera de línea se elimine de la vista. Para obtener más información, consulte "Recurso de suscripción de agente" en la página 1109.

Recuerde: Si el recopilador de datos ha proporcionado datos de rastreo de transacciones al Servidor de Cloud APM, la Consola de Cloud APM podría continuar mostrando el recopilador de datos en la aplicación **Mis componentes** y mostrar el mensaje de `El agente no es válido` para el recopilador de datos cuando haya caducado el periodo de tiempo especificado por el valor **Eliminar retardo de sistema fuera de línea**. Si ha instalado Cloud APM 8.1.4.0 Server con el arreglo temporal 3 o posterior, en última instancia un recopilador de datos no válido se eliminará de la aplicación **Mis componentes** 8 días después de que se dejen de recibir datos de rastreo de transacciones del recopilador de datos.

Configuración de la supervisión de Amazon EC2

Agente de Amazon EC2 le proporciona un punto central de supervisión del estado, disponibilidad y rendimiento de las instancias de Amazon Elastic Compute Cloud (EC2). El agente muestra un conjunto de métricas integral para ayudarle a tomar decisiones informadas sobre el entorno de EC2. Estas métricas incluyen el uso de CPU, el uso de Elastic Block Store (EBS), el uso de red, las actualizaciones de mantenimiento de Amazon Web Services (AWS) y el rendimiento de disco.

Antes de empezar

- Lea todo el tema "Configuración de la supervisión de Amazon EC2" en la página 197 para determinar qué se necesita para completar la configuración.
- Las instrucciones siguientes son para el release más reciente del agente, a excepción de lo indicado.
- Asegúrese de que los requisitos del sistema del Agente de Amazon EC2 se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Amazon EC2.
- Asegúrese de que la siguiente información está disponible:
  - Una lista de nombres de región de AWS que contienen instancias de EC2 a supervisar.
  - Las credenciales de seguridad de AWS (ID de clave de acceso y Clave de acceso secreta) con permiso para acceder a cada región de AWS.
- Asegúrese de que las credenciales de seguridad de AWS utilizadas para cada región de AWS son un miembro de un grupo que incluye como mínimo la política *AmazonEC2ReadOnlyAccess*.

Acerca de esta tarea

El Agente de Amazon EC2 es un agente de varias instancias y también un agente de subnodo. Puede crear una instancia de agente con varios subnodos, uno para cada región de Amazon EC2 o puede crear una instancia de agente para cada región de Amazon EC2 con un subnodo para esa región. También puede crear una combinación de cada tipo de configuración. Después de configurar instancias de agente, debe iniciar manualmente cada instancia de agente. Si tiene más de 50 recursos por región de Amazon EC2, se sugiere que cree una instancia de agente por región o que utilice el etiquetado en las instancias de EC2 y filtre las instancias de agente por las etiquetas creadas mediante el parámetro Condición de filtrado.

Procedimiento

1. Configure el agente en sistemas Windows mediante la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
   - "Configuración del agente en sistemas Windows" en la página 198.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 202.
2. Configure el agente en sistemas Linux con el script que solicita respuestas o el archivo de respuestas silencioso.
   - "Configuración del agente respondiendo a solicitudes" en la página 201.

- “Configuración del agente mediante el archivo de respuestas silencioso” en la página 202.

Qué hacer a continuación

En la Consola de Cloud APM, vaya al Panel de instrumentos del rendimiento de aplicaciones para ver los datos que se han recopilado. Para obtener más información sobre la utilización de la Consola de Cloud APM, consulte “Inicio de la Consola de Cloud APM” en la página 1009.

Si no puede ver los datos en los paneles de instrumentos del agente, consulte primero los registros de conexión del servidor y, a continuación, los registros del proveedor de datos. Las vías de acceso a estos registros se listan aquí:

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Si desea recibir ayuda con la resolución de problemas, consulte el Foro de Cloud Application Performance Management.

Configuración del agente en sistemas Windows

Puede configurar el Agente de Amazon EC2 en sistemas operativos Windows utilizando la ventana de IBM Cloud Application Performance Management. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la plantilla **Monitoring Agent for Amazon EC2** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar una instancia de agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar la instancia de agente de nuevo, púlsela con el botón derecho del ratón y luego pulse **Reconfigurar**.
3. Especifique un nombre de instancia exclusivo y luego pulse **Aceptar**. Utilice solo letras latinas, números arábigos y el carácter de guión o signo menos en el nombre de instancia. Por ejemplo, `ec2-inst3`.

Figura 3. La ventana para especificar un nombre de instancia exclusivo.

4. Pulse **Siguiente** en la ventana de nombre de instancia de agente.

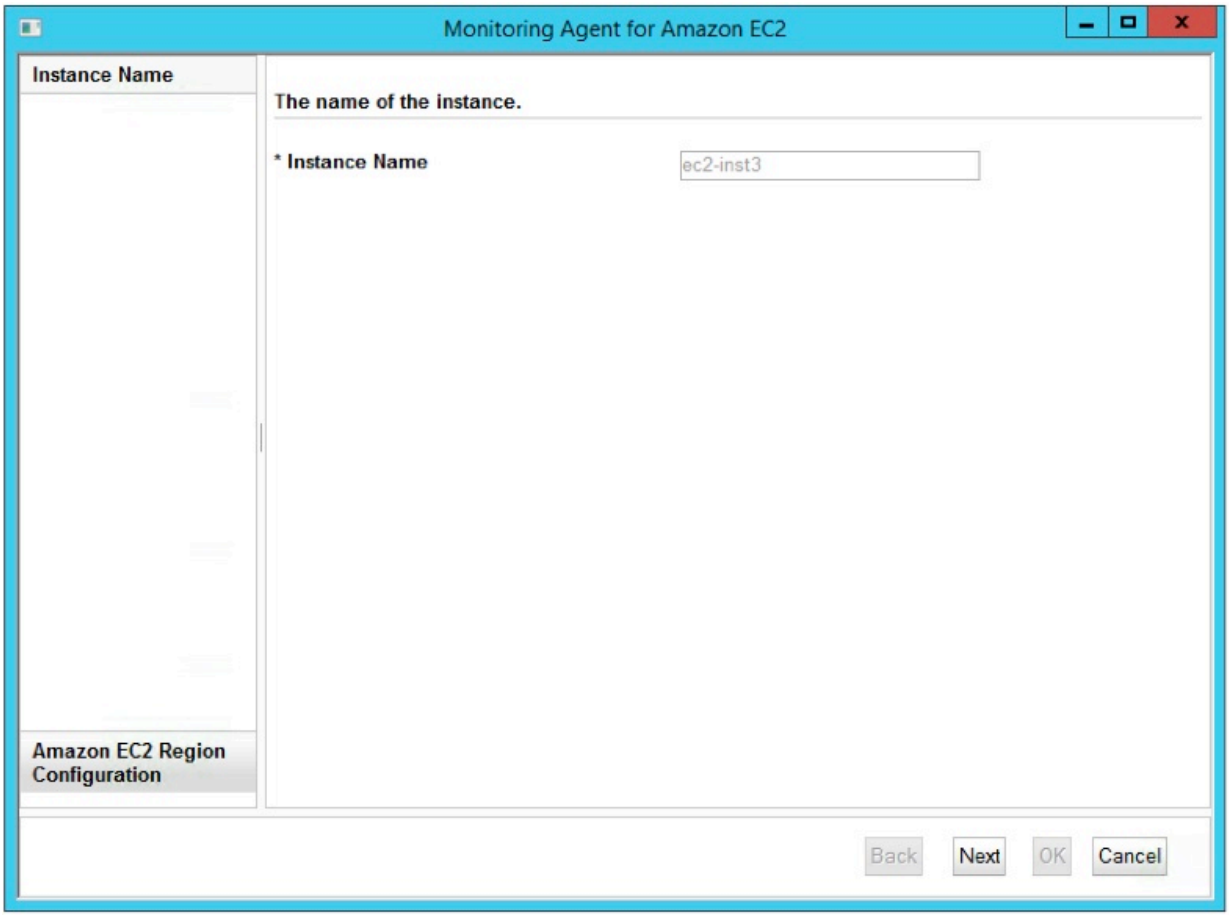


Figura 4. La ventana de nombre de instancia de agente.

5. Especifique los valores de la plantilla de instancia de **Configuración de región de Amazon EC2**.

   Nota: esta sección no corresponde a la configuración de instancia de región de Amazon EC2. Es una sección de la plantilla destinada a los valores que se utilizan como valores predeterminados al añadir las configuraciones de instancia de región de Amazon EC2 en el paso 6.

   Consulte la sección Tabla 14 en la página 203 para obtener una descripción de cada uno de los parámetros de configuración.

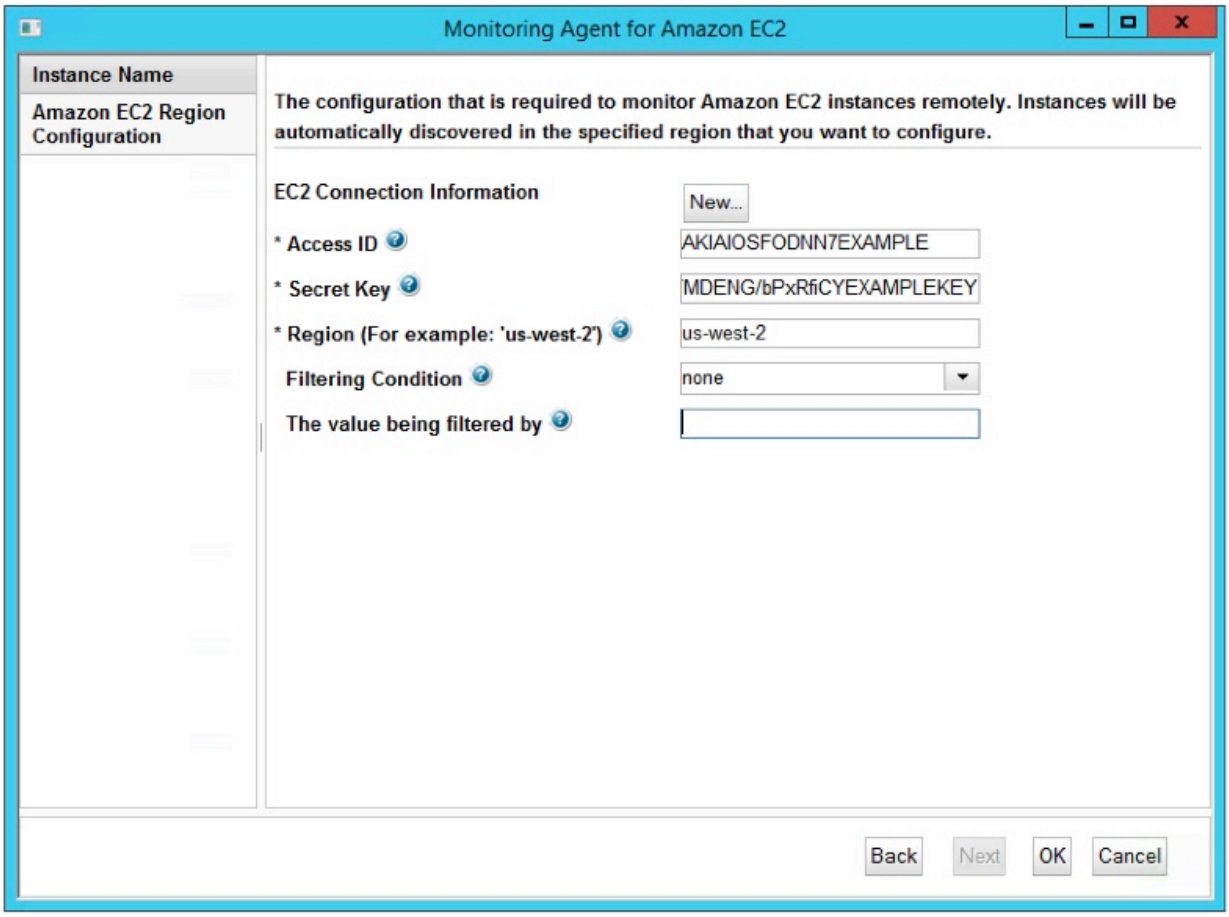


Figura 5. La ventana para especificar valores de plantilla de instancia de región de Amazon EC2.

6. Pulse **Nuevo** y especifique los valores de instancia de región de Amazon EC2. A continuación, pulse **Siguiente**.

   Consulte Tabla 14 en la página 203 para obtener una descripción de cada uno de los parámetros de configuración.

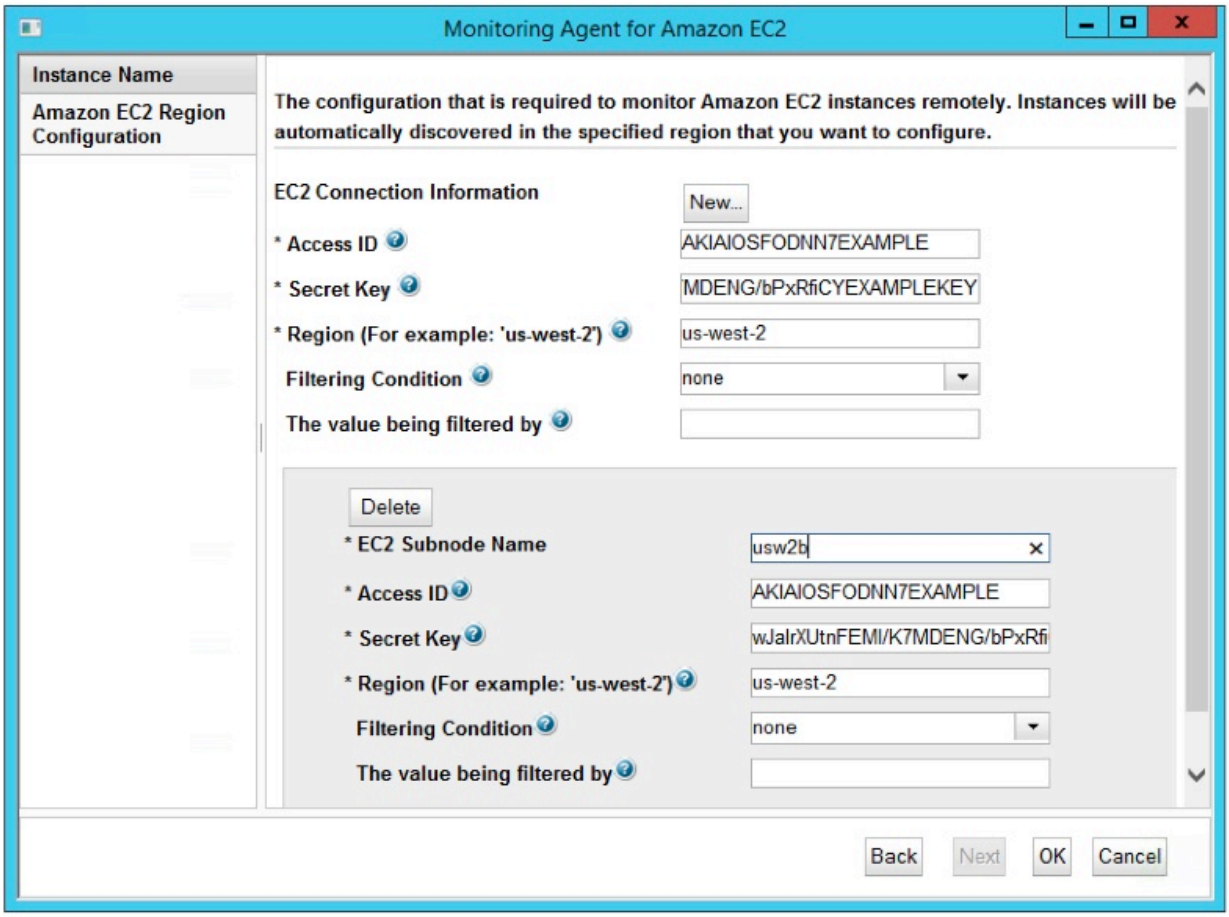


Figura 6. La ventana para especificar valores de instancia de región de Amazon EC2.

7. Pulse **Aceptar** para completar la configuración.
8. En la ventana de IBM Cloud Application Performance Management, pulse con el botón derecho del ratón la instancia que ha configurado y luego pulse **Iniciar**.

Configuración del agente respondiendo a solicitudes

Después de la instalación del Agente de Amazon EC2, debe configurarlo para poder iniciar el agente. Si el Agente de Amazon EC2 está instalado en un sistema Linux local, puede seguir estas instrucciones para configurarlo interactivamente a través de solicitudes de línea de mandatos.

Acerca de esta tarea

Recuerde: Si está volviendo a configurar una instancia de agente configurada, se visualiza el valor que se establece en la última configuración para cada opción. Si desea borrar un valor existente, pulse la tecla de espacio cuando se visualice el valor.

Procedimiento

Siga estos pasos para configurar el Agente de Amazon EC2 ejecutando un script y respondiendo a solicitudes.

1. Ejecute el mandato siguiente:

```
dir_instalación/bin/amazonec2-agent.sh config
nombre_instancia
```

donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

Ejemplo

```
/opt/ibm/apm/agent/bin/amazonec2-agent.sh config ec2-inst3
```

2. Responda a las solicitudes para establecer valores de configuración para el agente.

   Consulte la sección "Parámetros de configuración para el Agente de Amazon EC2" en la página 203 para obtener una descripción de cada uno de los parámetros de configuración.

3. Ejecute el mandato siguiente para iniciar el agente:

   ```
   dir_instalación/bin/amazonec2-agent.sh start
   nombre_instancia
   ```

   Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/amazonec2-agent.sh start ec2-inst3
   ```

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

- Configure el Agente de Amazon EC2 en modalidad silenciosa:
  a) En un editor de texto, abra el archivo `amazonec2_silent_config.txt` en una de las vías de acceso siguientes.
     – Linux *dir_instalación*`/samples/amazonec2_silent_config.txt`

       Por ejemplo, `/opt/ibm/apm/agent/samples/amazonec2_silent_config.txt`
     – Windows *dir_instalación*`\samples\amazonec2_silent_config.txt`

       Por ejemplo, `C:\IBM\APM\samples\amazonec2_silent_config.txt`

     Donde *dir_instalación* es la vía de acceso donde está instalado el agente.
  b) En el archivo `amazonec2_silent_config.txt` especifique valores para todos los parámetros obligatorios y modifique los valores predeterminados de otros parámetros según sea necesario.

     Consulte "Parámetros de configuración para el Agente de Amazon EC2" en la página 203 para obtener una descripción de cada uno de los parámetros de configuración.
  c) Guarde y cierre el archivo `amazonec2_silent_config.txt` y ejecute el mandato siguiente:
     – Linux *dir_instalación*`/bin/amazonec2-agent.sh config` **nombre_instancia** *dir_instalación*`/samples/amazonec2_silent_config.txt`

       Por ejemplo, **/opt/ibm/apm/agent/bin/amazonec2-agent.sh config ec2-inst3 /opt/ibm/apm/agent/samples/amazonec2_silent_config.txt**
     – Windows *dir_instalación*`\bin\amazonec2-agent.bat config` **nombre_instancia** *dir_instalación*`\samples\amazonec2_silent_config.txt`

Por ejemplo, **C:\IBM\APM\bin\amazonec2-agent.bat config ec2-inst3 C:\IBM\APM\samples\amazonec2_silent_config.txt**

Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

Importante: asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

d) Ejecute el mandato siguiente para iniciar el agente:

– Linux *dir_instalación*/bin/amazonec2-agent.sh start **nombre_instancia**

Por ejemplo, **/opt/ibm/apm/agent/bin/amazonec2-agent.sh start ec2-inst3**

– Windows *dir_instalación*\bin\amazonec2-agent.bat start **nombre_instancia**

Por ejemplo, **C:\IBM\APM\bin\amazonec2-agent.bat start ec2-inst3**

Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

Parámetros de configuración para el Agente de Amazon EC2

Los parámetros de configuración del Agente de Amazon EC2 se visualizan en una tabla.

1. Configuración de región de Amazon EC2: Valores para supervisar remotamente instancias de Amazon EC2. Las instancias se descubren automáticamente en la región especificada que desea configurar.

Tabla 14. Configuración de la región de Amazon EC2

Nombre de parámetro	Descripción	Nombre de parámetro del archivo de configuración silenciosa
Nombre de subnodo de EC2	Nombre del subnodo de EC2 para la recopilación de datos. Ejemplo, *usw2a*. Este alias forma parte del nombre de sistema gestionado (MSN) y se utiliza para identificar visualmente el entorno supervisado en la Consola de Cloud APM. **Nota:** Este alias puede ser cualquier cosa que elija para representar la instancia del subnodo de Amazon EC2 con las restricciones siguientes. Se pueden utilizar letras del alfabeto latino (a-z, A-Z), números arábigos (0-9), el carácter de guión o signo menos (-) y el carácter de subrayado (_) para crear nombres de instancia de subnodo de agente. La longitud máxima de un nombre de subnodo de EC2 es de 25 caracteres-	Cada uno de los parámetros siguientes debe tener un sufijo de nombre de subnodo de agente que sea el mismo para cada parámetro de una instancia de agente. Las instancias de subnodo de agente nuevas deben utilizar un nombre exclusivo para su conjunto de parámetros. Por ejemplo, una instancia de subnodo de agente puede utilizar *.usw2a* y otra instancia de subnodo de agente puede utilizar *.usw2b* en lugar de *.nombre_subnodo* en los nombres de parámetro siguientes.
ID de acceso	ID de clave de acceso de credenciales de seguridad AWS que se utiliza para autenticar con la región de Amazon especificada. Por ejemplo, 'AKIAxxxxxxxxxxxxxx'.	**KB5_INS_ACCESS_ID.nombre_subnodo**
Clave secreta	Clave de acceso secreta de credenciales de seguridad AWS que se utiliza para autenticar con la región de Amazon especificada. Por ejemplo, 'kK7txxxxxxxxxxxxxxxxxxxxxxxx'.	**KB5_INS_SECRET_KEY.nombre_subnodo**

Tabla 14. Configuración de la región de Amazon EC2 (continuación)

Nombre de parámetro	Descripción	Nombre de parámetro del archivo de configuración silenciosa
Región	Región de AWS a supervisar. Por ejemplo, 'us-west-2'.	**KB5_INS_REGION.nombre_subnodo**
Condición de filtrado	El tipo de filtrado que se está realizando. Puede utilizar etiquetas personalizadas en instancias de EC2 para limitar las instancias de EC2 que supervisa el atente. Para obtener más información, consulte Tagging Your Amazon EC2 Resources. Opciones de filtrado. **none** Se supervisan todas las instancias de EC2 dentro de la región. Se ignora el **Valor de filtro**. **tagName** Se supervisan las instancias de EC2 cuyas claves de etiqueta especificadas en **Valor de filtro**, independientemente del valor real de la etiqueta de instancia de correspondiente. Por ejemplo, para supervisar todas las instancias de EC2 cuya clave de etiqueta es *Stack*, independientemente del valor de la etiqueta, especifique `Stack` en **Valor de filtro**. **tagName|tagValue** Se supervisan las instancias de EC2 con el par de clave de etiqueta y de valor de etiqueta separado por una barra vertical (|) y especificado en el **Valor de filtro**. Por ejemplo, para supervisar todas las instancias de EC2 con la clave de etiqueta *Stack* y el valor de etiqueta *Production*, especifique `Stack|Production` en **Valor de filtro**. **monitoring-tag** Se supervisan las instancias de EC2 que tienen una etiqueta como mínimo. Se ignora el **Valor de filtro**.	**FILTER_CONDITION.nombre_subnodo** Valores válidos, **none** none **tagName** tagName **tagName|tagValue** tagName|tagValue **monitoring-tag** monitoring-tag
Valor de filtro	El valor de la etiqueta por la que se filtran las instancias de EC2 cuando `tagName` o `tagName|tagValue` están seleccionados para **Condición de filtrado**.	**FILTER_VALUE.nombre_subnodo**

Configuración de la supervisión del Equilibrador de carga elástico de AWS

El Agente de Amazon ELB proporciona un punto central de supervisión del estado, la disponibilidad y el rendimiento de los Equilibradores de carga elásticos de AWS. El agente muestra un conjunto exhaustivo de métricas para cada aplicación de tipo equilibrador de carga, ayuda de red y clásica para ayudarle a tomar decisiones sobre su entorno de Equilibrador de carga elástico de AWS basadas en información.

Antes de empezar

- Lea todo el tema "Configuración de la supervisión del Equilibrador de carga elástico de AWS" en la página 205 para determinar qué se necesita para completar la configuración.
- Las instrucciones siguientes son para el release más reciente del agente, a excepción de lo indicado.
- Asegúrese de que los requisitos del sistema del Agente de Amazon ELB se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Amazon ELB.
- Asegúrese de que la siguiente información está disponible:
  - Las credenciales de seguridad de AWS (ID de clave de acceso y Clave de acceso secreta) con permiso para acceder a cada región de AWS con Equilibradores de carga elásticos.

Acerca de esta tarea

El Agente de Amazon ELB es un agente de varias instancias y también un agente de subnodo. Se crean automáticamente subnodos para cada tipo de Equilibrador de carga elástico disponible en el entorno de AWS.

Procedimiento

1. Configure el agente en sistemas Windows mediante la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
   - "Configuración del agente en sistemas Windows" en la página 206.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 208.
2. Configure el agente en sistemas Linux con el script que solicita respuestas o el archivo de respuestas silencioso.
   - "Configuración del agente respondiendo a solicitudes" en la página 207.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 208.

Qué hacer a continuación

En la Consola de Cloud APM, vaya al Panel de instrumentos del rendimiento de aplicaciones para ver los datos que se han recopilado. Para obtener más información sobre la utilización de la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si no puede ver los datos en los paneles de instrumentos del agente, consulte primero los registros de conexión del servidor y, a continuación, los registros del proveedor de datos. Las vías de acceso a estos registros se listan aquí:

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Si desea recibir ayuda con la resolución de problemas, consulte el Foro de Cloud Application Performance Management.

Configuración del agente en sistemas Windows

Puede configurar el Agente de Amazon ELB en sistemas operativos Windows utilizando la ventana de IBM Cloud Application Performance Management. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la plantilla **Monitoring Agent for AWS Elastic Load Balancer** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar una instancia de agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar la instancia de agente de nuevo, púlsela con el botón derecho del ratón y luego pulse **Reconfigurar**.
3. Especifique un nombre de instancia exclusivo y luego pulse **Aceptar**. Utilice solo letras latinas, números arábigos y el carácter de guión o signo menos en el nombre de instancia. Ejemplo, `elb-inst3`. Para obtener más información, consulte *nombre_instancia* en "Formato común de MSN para agentes de varias instancias" en la página 174.

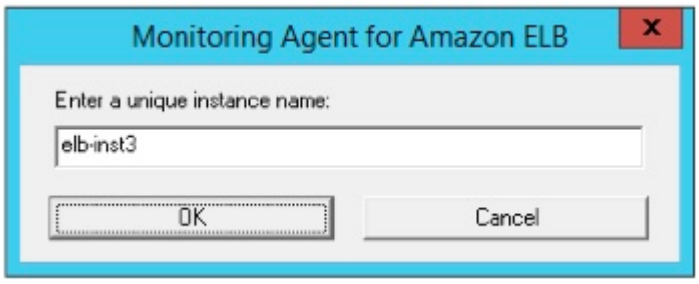


Figura 7. La ventana para indicar un nombre de instancia de agente exclusivo.

4. Escriba las **Credenciales de suscripción de Amazon ELB** y, a continuación, pulse **Siguiente**.

   Consulte "Parámetros de configuración para el Agente de Amazon ELB" en la página 209 para obtener una descripción de cada uno de los parámetros de configuración.

   Importante: Windows Si la **`Clave secreta o contraseña`** contiene un signo igual (=), debe escribirla de nuevo cada vez que vuelva a configurar el agente.

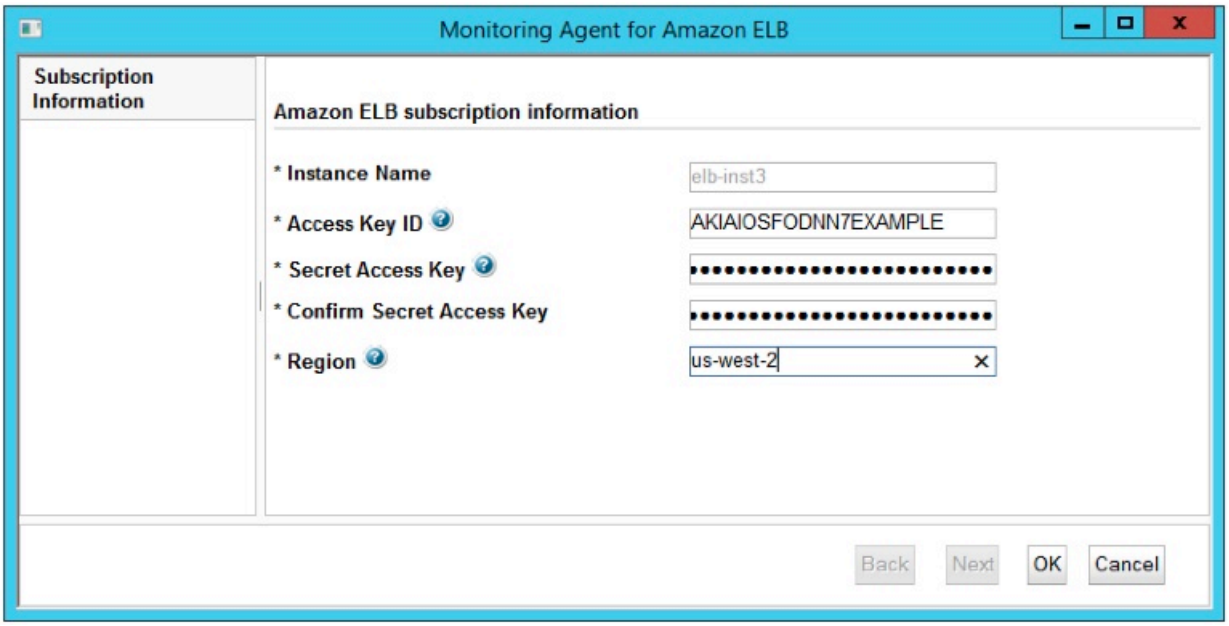


Figura 8. La ventana Credenciales de suscripción de Amazon ELB.

5. Pulse **Aceptar** para completar la configuración.
6. En la ventana de IBM Cloud Application Performance Management, pulse con el botón derecho del ratón la instancia que ha configurado y luego pulse **Iniciar**.

Configuración del agente respondiendo a solicitudes

Después de la instalación del Agente de Amazon ELB, debe configurarlo para poder iniciar el agente. Si el Agente de Amazon ELB está instalado en un sistema Linux local, puede seguir estas instrucciones para configurarlo interactivamente a través de solicitudes de línea de mandatos.

Acerca de esta tarea

Recuerde: Si está volviendo a configurar una instancia de agente configurada, se visualiza el valor que se establece en la última configuración para cada opción. Si desea borrar un valor existente, pulse la tecla de espacio cuando se visualice el valor.

Procedimiento

Siga estos pasos para configurar el Agente de Amazon ELB ejecutando un script y respondiendo a solicitudes.

1. Ejecute el mandato siguiente:

   ```
   dir_instalación/bin/amazon_elb-agent.sh config nombre_instancia
   ```

   Donde *dir_instalación* es la vía de acceso donde se ha instalado el agente y *nombre_instancia* es el nombre que desea otorgar a la instancia del agente. Utilice solamente latinas, números arábigos y el carácter de guión o signo menos en el *nombre_instancia*. Para obtener más información, consulte *nombre_instancia* en “Formato común de MSN para agentes de varias instancias” en la página 174.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/amazon_elb-agent.sh config elb-inst3
   ```

2. Responda a las solicitudes para establecer valores de configuración para el agente.

   Consulte la sección “Parámetros de configuración para el Agente de Amazon ELB” en la página 209 para obtener una descripción de cada uno de los parámetros de configuración.

3. Ejecute el mandato siguiente para iniciar el agente:

   ```
   dir_instalación/bin/amazon_elb-agent.sh start nombre_instancia
   ```

   Siendo *dir_instalación* la vía de acceso donde se ha instalado el agente y *nombre_instancia* es el nombre de la instancia del agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/amazon_elb-agent.sh start elb-inst3
   ```

Ejemplo

Creación de una instancia de agente denominada `elb-inst3`.

```
# ./amazon_elb-agent.sh config elb-inst3
Configuración de Monitoring Agent for Amazon ELB

¿Desea editar los valores de "Monitoring Agent for Amazon ELB"? [1=Sí,2=No] (valor
predeterminado: 1): 1

Información de suscripción:
Información de suscripción de Amazon ELB

El ID de acceso utilizado para autenticar con la región de Amazon especificada.
Información de suscripción:
ID de clave de acceso (el valor predeterminado es: ): AKIAIOSFODNN7EXAMPLE
```

```
La clave de acceso secreta utilizada para autenticar con la región de Amazon
especificada. Por ejemplo, 'kK7txxxxxxxxxxxxxxxxxxxxxxxx'.
Escriba la clave de acceso secreta (el valor predeterminado es:): hidden

Vuelva a escribir: Clave de acceso secreta (el valor predeterminado es:): hidden

La región de Amazon en la que los equilibradores de carga están ubicados. Por ejemplo, 'us-
west-2'.
Región (el valor predeterminado es: ): us-west-2

La configuración se ha completado satisfactoriamente.
Se ha configurado el inicio automático en la inicialización de sistema.
Se ha configurado la detención automática al concluir el sistema.
```

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

Siga estos pasos para configurar el Agente de Amazon ELB en modalidad silenciosa.

1. En un editor de texto, abra el archivo `amazon_elb_silent_config.txt` en una de las vías de acceso siguientes.
   - Linux *dir_instalación*`/samples/amazon_elb_silent_config.txt`

     Ejemplo, `/opt/ibm/apm/agent/samples/amazon_elb_silent_config.txt`
   - Windows *dir_instalación*`\samples\amazon_elb_silent_config.txt`

     Ejemplo, `C:\IBM\APM\samples\amazon_elb_silent_config.txt`

   Donde *dir_instalación* es la vía de acceso donde se ha instalado el agente.
2. En el archivo `amazon_elb_silent_config.txt` especifique valores para todos los parámetros obligatorios y modifique los valores predeterminados de otros parámetros según sea necesario.

   Consulte “Parámetros de configuración para el Agente de Amazon ELB” en la página 209 para obtener una descripción de cada uno de los parámetros de configuración.
3. Guarde y cierre el archivo `amazon_elb_silent_config.txt` y ejecute el mandato siguiente:
   - Linux *dir_instalación*`/bin/amazon_elb-agent.sh config` **nombre_instancia** *dir_instalación*`/samples/amazon_elb_silent_config.txt`

     Ejemplo, **`/opt/ibm/apm/agent/bin/amazon_elb-agent.sh config elb-inst3 /opt/ibm/apm/agent/samples/amazon_elb_silent_config.txt`**
   - Windows *dir_instalación*`\bin\amazon_elb-agent.bat config` **nombre_instancia** *dir_instalación*`\samples\amazon_elb_silent_config.txt`

     Ejemplo, **`C:\IBM\APM\bin\amazon_elb-agent.bat config elb-inst3 C:\IBM\APM\samples\amazon_elb_silent_config.txt`**

   Donde *dir_instalación* es la vía de acceso donde se ha instalado el agente y *nombre_instancia* es el nombre que desea otorgar a la instancia del agente. Utilice solamente latinas, números arábigos y el

carácter de guión o signo menos en el *nombre_instancia*. Para obtener más información, consulte *nombre_instancia* en "Formato común de MSN para agentes de varias instancias" en la página 174.

Importante: Asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

4. Ejecute el mandato siguiente para iniciar el agente:
   - Linux *dir_instalación*/bin/amazon_elb-agent.sh start **nombre_instancia**

     Ejemplo, **/opt/ibm/apm/agent/bin/amazon_elb-agent.sh start elb-inst3**
   - Windows *dir_instalación*\bin\amazon_elb-agent.bat start **nombre_instancia**

     Ejemplo, **C:\IBM\APM\bin\amazon_elb-agent.bat start elb-inst3**

   Siendo *dir_instalación* la vía de acceso donde se ha instalado el agente y *nombre_instancia* es el nombre de la instancia del agente.

Ejemplo

Archivo amazon_elb_silent_config.txt editado.

```
#
# Este es un archivo de respuesta de configuración de ejemplo para el agente Amazon ELB.
#
# Contiene una entrada para cada propiedad de configuración.
# Las entradas para propiedades opcionales que no tienen ningún valor predeterminado
# se incluyen en los comentarios.
# Asegúrese de que todas las propiedades descomentadas tengan un valor antes de configurar el
# agente.
#

# ID de clave de acceso: El ID de acceso utilizado para autenticar con la
# región de Amazon especificada. Por ejemplo, 'AKIAxxxxxxxxxxxxxx'.
KAL_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

# Clave de acceso secreta: La clave de acceso secreta utilizada para autenticar con
# la región de Amazon especificada. Por ejemplo, 'kK7txxxxxxxxxxxxxxxxxxxxxxxx'.
KAL_SECRET_ACCESS_KEY_PASSWORD=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

# Región: La región de Amazon en la que los equilibradores de carga están ubicados. Por
# ejemplo, 'us-west-2'.
KAL_REGION=us-west-2
```

Parámetros de configuración para el Agente de Amazon ELB

Los parámetros de configuración del Agente de Amazon ELB se visualizan en una tabla.

1. Tabla 15 en la página 209: Credenciales necesarias para acceder a la suscripción de Amazon que contiene los recursos de Equilibradores de carga elásticos que se han de supervisar.

Tabla 15. Información de suscripción

Nombre de parámetro	Descripción	Nombre de parámetro del archivo de configuración silenciosa
ID de clave de acceso	El ID de acceso utilizado para autenticar con la región de Amazon especificada. Por ejemplo, 'AKIAxxxxxxxxxxxxxx'.	**KAL_ACCESS_KEY_ID**
Clave de acceso secreta	La clave de acceso secreta utilizada para autenticar con la región de Amazon especificada. Por ejemplo, 'kK7txxxxxxxxxxxxxxxxxxxxxxxx'.	**KAL_SECRET_ACCESS_KEY_PASSWORD**
Región	La región de Amazon en la que los equilibradores de carga están ubicados. Por ejemplo, 'us-west-2'.	**KAL_REGION**

Configuración de la supervisión de Azure Compute

El Agente de Azure Compute proporciona un punto central de supervisión del estado, la disponibilidad y el rendimiento de las instancias de Azure Compute. El agente muestra un conjunto de métricas integral para ayudarle a tomar decisiones informadas sobre el entorno de Azure Compute. Estas métricas incluyen el uso de CPU, el uso de red y el rendimiento de disco.

Antes de empezar

- Lea todo el tema "Configuración de la supervisión de Azure Compute" en la página 210 para determinar qué se necesita para completar la configuración.
- Las instrucciones siguientes son para el release más reciente del agente, a excepción de lo indicado.
- Asegúrese de que los requisitos del sistema del Agente de Azure Compute se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Azure Compute.
- Asegúrese de que la siguiente información está disponible:
  - Las credenciales de suscripción de Azure con permiso para acceder a las instancia de Azure Compute que se han de supervisar.Consulte "Información de configuración de Azure Compute" en la página 211 para obtener más información.

Acerca de esta tarea

El Agente de Azure Compute es un agente de varias instancias y también un agente de subnodo. Cada subnodo de Agente de Azure Compute supervisa una agrupación de máquinas virtuales de Azure Compute en función de un filtro que se defina. Puede crear una instancia de agente con varios subnodos, uno para cada agrupación de máquina virtual, o puede crear una instancia de agente para cada agrupación de máquina virtual con un subnodo para esa agrupación. También puede crear una combinación de cada tipo de configuración. Después de configurar instancias de agente, debe iniciar manualmente cada instancia de agente. Se sugiere no tener más de 50 recursos por agrupación de máquina virtual de Azure Compute. Cada nombre de subnodo de Azure Compute debe ser exclusivo en su entorno.

Procedimiento

1. Configure el agente en sistemas Windows mediante la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
   - "Configuración del agente en sistemas Windows" en la página 211.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 216.
2. Configure el agente en sistemas Linux con el script que solicita respuestas o el archivo de respuestas silencioso.
   - "Configuración del agente respondiendo a solicitudes" en la página 214.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 216.

Qué hacer a continuación

En la Consola de Cloud APM, vaya al Panel de instrumentos del rendimiento de aplicaciones para ver los datos que se han recopilado. Para obtener más información sobre la utilización de la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si no puede ver los datos en los paneles de instrumentos del agente, consulte primero los registros de conexión del servidor y, a continuación, los registros del proveedor de datos. Las vías de acceso a estos registros se listan aquí:

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Si desea recibir ayuda con la resolución de problemas, consulte el Foro de Cloud Application Performance Management.

Información de configuración de Azure Compute

El Agente de Azure Compute requiere la configuración adicional en el entorno de Azure Compute.

Acerca de esta tarea

Para ejecutar estos pasos, debe iniciar la sesión en la consola de Microsoft Azure.

Procedimiento

1. ID de suscripción
   - En el panel de la izquierda, seleccione "Suscripciones" y elija la suscripción que desea utilizar para este agente.
   - Seleccione "Visión general" y, a continuación, copie el ID de suscripción. Esto se utilizará como uno de los parámetros de configuración del agente.
2. ID de arrendatario
   - Vaya al "Directorio de Azure Active".
   - Seleccione "Propiedades" y, a continuación, copie el ID de arrendatario.
3. Registre una aplicación
   - Vaya a "Todos los servicios" y busque "Registros de aplicación".
   - Pulse "Nuevo registro de aplicación".
   - Rellene un nombre, seleccione el Tipo de aplicación "Web App/API" y un URL de inicio de sesión (este URL no se utilizará por lo que puede elegir lo que desee).
   - Pulse "Crear"
   - Copie el ID de aplicación: este se utilizará en el campo "ID de cliente" del agente.
4. Cree una clave de aplicación
   - Pulse en la aplicación que acaba de crear y, a continuación, vaya a "Valores" seguido de "Claves".
   - Escriba una descripción (por ejemplo, "Clave de IBM") y una duración (por ejemplo, "Nunca caduca") y luego pulse "Guardar".
   - Copie la clave Secreta y almacénela en algún lugar seguro; solo verá esta clave una vez y tendrá que generar una nueva si lo pierde.
5. Otorgue los permisos de aplicación
   - Vaya a "Suscripciones" y seleccione la suscripción que se va a supervisar.
   - Vaya a "Control de acceso" (IAM) y pulse "Añadir".
   - Seleccione el rol "Lector" o superior para la supervisión.
   - En "Seleccionar", busque la aplicación que acaba de registrar y selecciónela; a continuación, pulse "Guardar".

Configuración del agente en sistemas Windows

Puede configurar el Agente de Azure Compute en sistemas operativos Windows utilizando la ventana de IBM Cloud Application Performance Management. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la plantilla **Monitoring Agent for Azure Compute** y luego pulse **Configurar agente**.

Recuerde: Después de configurar una instancia de agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar la instancia de agente de nuevo, púlsela con el botón derecho del ratón y luego pulse **Reconfigurar**.

3. Especifique un nombre de instancia exclusivo y luego pulse **Aceptar**. Utilice solo letras latinas, números arábigos y el carácter de guión o signo menos en el nombre de instancia. Por ejemplo, `azc-inst3`. Para obtener más información, consulte *nombre_instancia* en "Formato común de MSN para agentes de varias instancias" en la página 174.

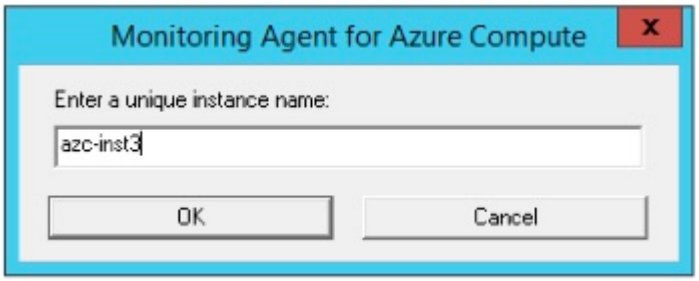


Figura 9. La ventana para indicar un nombre de instancia de agente exclusivo.

4. Escriba las **Credenciales de suscripción de Azure** y, a continuación, pulse **Siguiente**.

   Consulte la sección Tabla 16 en la página 218 para obtener una descripción de cada uno de los parámetros de configuración.

   Importante: Windows Si la **`Clave secreta o contraseña`** contiene un signo igual (=), debe escribirla de nuevo cada vez que vuelva a configurar el agente.

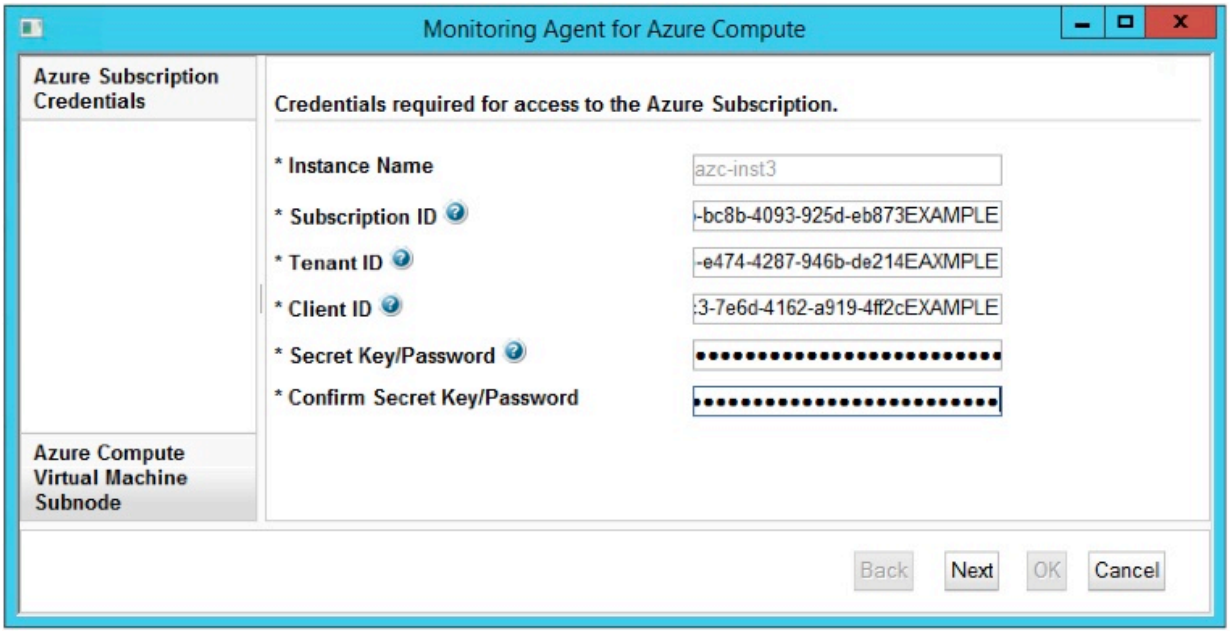


Figura 10. La ventana Credenciales de suscripción de Azure.

5. Escriba los valores de la plantilla **Subnodo de máquina virtual de Azure Compute**.

   Consulte la sección Tabla 17 en la página 219 para obtener una descripción de cada uno de los parámetros de configuración.

   Nota: Esta sección no es la configuración de la instancia Subnodo de máquina virtual de Azure Compute. Se trata de una sección de plantillas para establecer los valores que se utilizan como valores predeterminado cuando se añaden las configuraciones de instancia del Subnodo de máquina virtual de Azure Compute real en el paso 6.

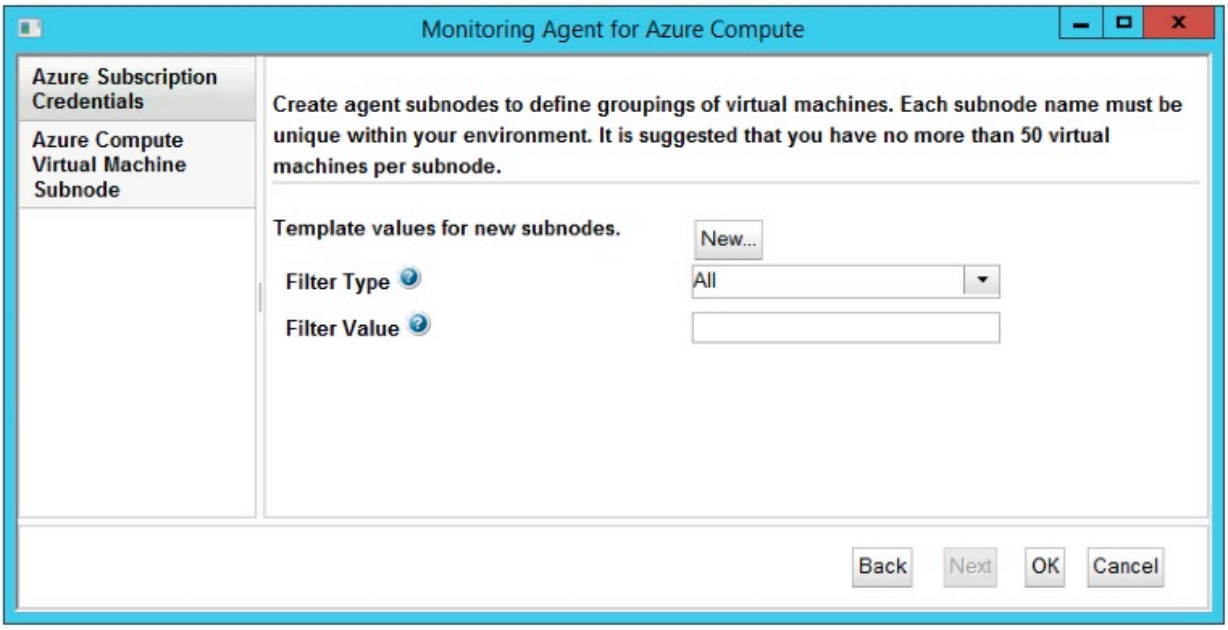


Figura 11. La ventana para especificar los valores de plantilla del Subnodo de máquina virtual de Azure Compute.

6. Pulse **Nuevo** y escriba los valores de instancia **Subnodo de máquina virtual de Azure Compute** y, a continuación, pulse **Siguiente**.

   Consulte la sección Tabla 17 en la página 219 para obtener una descripción de cada uno de los parámetros de configuración.

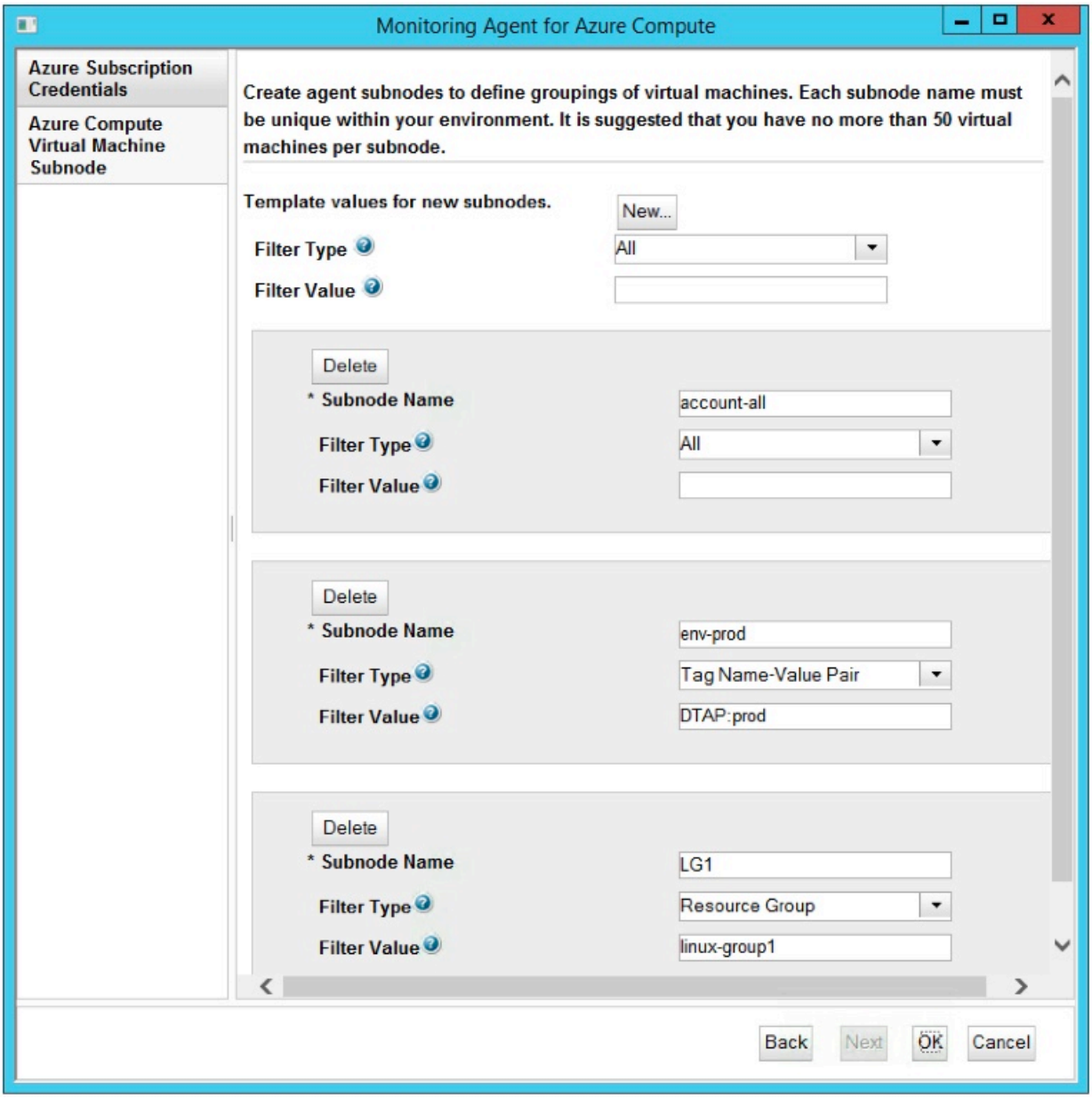


Figura 12. La ventana para especificar los valores de instancia del Subnodo de máquina virtual de Azure Compute.

7. Pulse **Aceptar** para completar la configuración.
8. En la ventana de IBM Cloud Application Performance Management, pulse con el botón derecho del ratón la instancia que ha configurado y luego pulse **Iniciar**.

Configuración del agente respondiendo a solicitudes

Después de la instalación del Agente de Azure Compute, debe configurarlo para poder iniciar el agente. Si el Agente de Azure Compute está instalado en un sistema Linux local, puede seguir estas instrucciones para configurarlo interactivamente a través de solicitudes de línea de mandatos.

Acerca de esta tarea

Recuerde: Si está volviendo a configurar una instancia de agente configurada, se visualiza el valor que se establece en la última configuración para cada opción. Si desea borrar un valor existente, pulse la tecla de espacio cuando se visualice el valor.

Procedimiento

Siga estos pasos para configurar el Agente de Azure Compute ejecutando un script y respondiendo a solicitudes.

1. Ejecute el mandato siguiente:

   ```
   dir_instalación/bin/azure_compute-agent.sh config nombre_instancia
   ```

   Donde *dir_instalación* es la vía de acceso donde se ha instalado el agente y *nombre_instancia* es el nombre que desea otorgar a la instancia del agente. Utilice solamente latinas, números arábigos y el carácter de guión o signo menos en el *nombre_instancia*. Para obtener más información, consulte *nombre_instancia* en "Formato común de MSN para agentes de varias instancias" en la página 174.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/azure_compute-agent.sh config azc-inst3
   ```

2. Responda a las solicitudes para establecer valores de configuración para el agente.

   Consulte la sección "Parámetros de configuración para el Agente de Azure Compute" en la página 218 para obtener una descripción de cada uno de los parámetros de configuración.

   Recuerde: La primera vez que configure una instancia de agente, deberá añadir como mínimo un subnodo cuando se le solicite **Edite los valores del "subnodo de la máquina virtual de Azure Compute"**.

3. Ejecute el mandato siguiente para iniciar el agente:

   ```
   dir_instalación/bin/azure_compute-agent.sh start nombre_instancia
   ```

   Siendo *dir_instalación* la vía de acceso donde se ha instalado el agente y *nombre_instancia* es el nombre de la instancia del agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/azure_compute-agent.sh start azc-inst3
   ```

Ejemplo

Creación de una instancia de agente denominada `azc-inst3` y que tiene una instancia de subnodo denominada `azc1`.

```
# ./azure_compute-agent.sh config azc-inst3
Configuración de Monitoring Agent for Azure Compute

¿Desea editar los valores de "Monitoring Agent for Azure Compute"? [1=Sí,2=No] (valor
predeterminado: 1): 1

Credenciales de suscripción de Azure:
Las credenciales necesarias para acceder a la suscripción de Azure.

El ID asignado por Azure para la suscripción que se supervisa.
ID de suscripción (el valor predeterminado es): 09x73b6b-bcxb-40x3-92xd-ebx7-EXAMPLE

El ID del arrendatario que ha asignado Azure. Se utiliza para iniciar sesión en la API de
servicio de Azure.
ID de arrendatario (el valor predeterminado es:): 75x2e745-e4x4-42x7-94xb-dex1-EXAMPLE

El ID de cliente que ha asignado Azure para identificar este agente como
aplicación externa que supervisa los servicios de cálculo de Azure.
ID de cliente (el valor predeterminado es:): 79x2e6c3-7exd-41x2-a9x9-4fx2-EXAMPLE

La clave de acceso secreta o contraseña que ha creado Azure para la aplicación cliente.
Escriba la clave secreta o la contraseña (el valor predeterminado es:): hidden

Vuelva a escribir: clave secreta o contraseña (el valor predeterminado es:): hidden

Subnodo de máquina virtual de Azure Compute:

Cree los subnodos de agente para definir agrupaciones de máquinas virtuales. Cada nombre de
subnodo
```

```
debe ser exclusivo en el entorno. Se sugiere no tener más de
50 máquinas virtuales por subnodo.

No hay disponibles valores de "subnodo de máquina virtual de Azure Compute".
Edite los valores del "Subnodo de máquina virtual de Azure Compute", [1=Añadir, 2=Editar,
3=Suprimir,
4=Siguiente, 5=Salir] (el valor predeterminado es: 5): 1
Nombre de subnodo (el valor predeterminado es:): azc1
El tipo de filtro que se debe aplicar.
Tipo de filtro [ 1=Todos, 2=Par de etiqueta nombre-valor, 3=Grupo de recursos ] (valor
predeterminado: 1): 2
El valor de filtro correspondiente al tipo de filtro seleccionado. Este valor puede ser un
Grupo de recursos o un Par de etiqueta nombre-valor, por ejemplo Entorno\:Producción.
Puede que aparezca una barra inclinada invertida en el ejemplo, no escriba ninguna
barra inclinada invertida en el valor que proporcione.
Valor de filtro (el valor predeterminado es: ): Entorno:Producción



Valores del subnodo de máquina virtual de Azure Compute: Nombre del subnodo=azc1
Edite los valores del "Subnodo de máquina virtual de Azure Compute", [1=Añadir, 2=Editar,
3=Suprimir,
4=Siguiente, 5=Salir] (el valor predeterminado es: 5): 5
La configuración se ha completado satisfactoriamente.
Se ha configurado el inicio automático en la inicialización de sistema.
Se ha configurado la detención automática al concluir el sistema.
Tiene correo nuevo en /var/spool/mail/root
```

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

Siga estos pasos para configurar el Agente de Azure Compute en modalidad silenciosa.

1. En un editor de texto, abra el archivo `azure_compute_silent_config.txt` en una de las vías de acceso siguientes.
   - Linux *dir_instalación*`/samples/azure_compute_silent_config.txt`

     Ejemplo, `/opt/ibm/apm/agent/samples/azure_compute_silent_config.txt`
   - Windows *dir_instalación*`\samples\azure_compute_silent_config.txt`

     Ejemplo, `C:\IBM\APM\samples\azure_compute_silent_config.txt`

   Donde *dir_instalación* es la vía de acceso donde se ha instalado el agente.
2. En el archivo `azure_compute_silent_config.txt` especifique valores para todos los parámetros obligatorios y modifique los valores predeterminados de otros parámetros según sea necesario.

   Consulte la sección “Parámetros de configuración para el Agente de Azure Compute” en la página 218 para obtener una descripción de cada uno de los parámetros de configuración.

   Importante: Debe habilitar y especificar los parámetros Tipo de filtro y Valor de filtro para como mínimo un nodo de subnodo.
3. Guarde y cierre el archivo `azure_compute_silent_config.txt` y ejecute el mandato siguiente:

- Linux *dir_instalación*/bin/azure_compute-agent.sh config **nombre_instancia** *dir_instalación*/samples/azure_compute_silent_config.txt

  Por ejemplo, **/opt/ibm/apm/agent/bin/azure_compute-agent.sh config azc-inst3 /opt/ibm/apm/agent/samples/azure_compute_silent_config.txt**

- Windows *dir_instalación*\bin\azure_compute-agent.bat config **nombre_instancia** *dir_instalación*\samples\azure_compute_silent_config.txt

  Por ejemplo, **C:\IBM\APM\bin\azure_compute-agent.bat config azc-inst3 C:\IBM\APM\samples\azure_compute_silent_config.txt**

Donde *dir_instalación* es la vía de acceso donde se ha instalado el agente y *nombre_instancia* es el nombre que desea otorgar a la instancia del agente. Utilice solamente latinas, números arábigos y el carácter de guión o signo menos en el *nombre_instancia*. Para obtener más información, consulte *nombre_instancia* en "Formato común de MSN para agentes de varias instancias" en la página 174.

Importante: Asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

4. Ejecute el mandato siguiente para iniciar el agente:

   - Linux *dir_instalación*/bin/azure_compute-agent.sh start **nombre_instancia**

     Por ejemplo, **/opt/ibm/apm/agent/bin/azure_compute-agent.sh start azc-inst3**

   - Windows *dir_instalación*\bin\azure_compute-agent.bat start **nombre_instancia**

     Por ejemplo, **C:\IBM\APM\bin\azure_compute-agent.bat start azc-inst3**

   Siendo *dir_instalación* la vía de acceso donde se ha instalado el agente y *nombre_instancia* es el nombre de la instancia del agente.

Ejemplo

azure_compute_silent_config.txt editado con tres subnodos que se denominan account-all, env-prod y LG1.

```
#
# Este es un archivo de respuesta de configuración de ejemplo para el agente Azure Compute.
#
# Contiene una entrada para cada propiedad de configuración.
# Las entradas para propiedades opcionales que no tienen ningún valor predeterminado
# se incluyen en los comentarios.
# A las entradas para el subnodo AVM se les da un nombre de instancia de subnodo de ejemplo de
avm1.
# Asegúrese de que todas las propiedades descomentadas tengan un valor antes de configurar el
# agente.
#

# ID de suscripción: El ID asignado por Azure para la suscripción que se
# supervisa.
KAK_SUBSCRIPTION_ID=09x73b6b-bcxb-40x3-92xd-ebx7-EXAMPLE
# ID de arrendatario: El ID del arrendatario que ha asignado Azure. Se utilizaba para
# iniciar sesión en la API del servicio de Azure.
KAK_TENANT_ID=75x2e745-e4x4-42x7-94xb-dex1-EXAMPLE
# ID de cliente: El ID del cliente asignado por Azure para identificar este agente
# como aplicación externa
# que supervisa los servicios de cálculo de Azure.
KAK_CLIENT_ID=79x2e6c3-7exd-41x2-a9x9-4fx2-EXAMPLE
# Clave secreta/Contraseña: La clave de acceso secreto o la contraseña que ha creado
# Azure para la aplicación cliente.
KAK_SECRET_PASSWORD=hZxWPq/IOxlnvg/wdxLwTf2Fs3x2sWQV/sCE-EXAMPLE

# Tipo de filtro: El tipo de filtro que se debe aplicar.
# Valores válidos: ALL (All), TAG_NAME_VALUE (Par de etiqueta nombre-valor),
# RESOURCE_GROUP (Grupo de recursos)
#KAK_FILTER_TYPE.avm1=ALL
# Valor de filtro: El valor de filtro correspondiente al tipo de filtro seleccionado.
# Este valor puede ser un Grupo de recursos o un Par de etiqueta nombre-valor, por ejemplo
# Environment:Production. Puede que aparezca una barra inclinada invertida en el ejemplo,
# no la escriba en el valor que proporcione.
#KAK_FILTER_VALUE.avm1=
```

```
# Tipo de filtro: El tipo de filtro que se debe aplicar.
# Valores válidos: ALL (All), TAG_NAME_VALUE (Par de etiqueta nombre-valor),
# RESOURCE_GROUP (Grupo de recursos)
KAK_FILTER_TYPE.account-all=ALL
# Valor de filtro: El valor de filtro correspondiente al tipo de filtro seleccionado.
# Este valor puede ser un Grupo de recursos o un Par de etiqueta nombre-valor, por ejemplo
# Environment:Production. Puede que aparezca una barra inclinada invertida en el ejemplo,
# no la escriba en el valor que proporcione.
KAK_FILTER_VALUE.account-all=

# Tipo de filtro: El tipo de filtro que se debe aplicar.
# Valores válidos: ALL (All), TAG_NAME_VALUE (Par de etiqueta nombre-valor),
# RESOURCE_GROUP (Grupo de recursos)
KAK_FILTER_TYPE.env-prod=TAG_NAME_VALUE
# Valor de filtro: El valor de filtro correspondiente al tipo de filtro seleccionado.
# Este valor puede ser un Grupo de recursos o un Par de etiqueta nombre-valor, por ejemplo
# Environment:Production. Puede que aparezca una barra inclinada invertida en el ejemplo,
# no la escriba en el valor que proporcione.
KAK_FILTER_VALUE.env-prod=DTAP:prod

# Tipo de filtro: El tipo de filtro que se debe aplicar.
# Valores válidos: ALL (All), TAG_NAME_VALUE (Par de etiqueta nombre-valor),
# RESOURCE_GROUP (Grupo de recursos)
KAK_FILTER_TYPE.LG1=RESOURCE_GROUP
# Valor de filtro: El valor de filtro correspondiente al tipo de filtro seleccionado.
# Este valor puede ser un Grupo de recursos o un Par de etiqueta nombre-valor, por ejemplo
# Environment:Production. Puede que aparezca una barra inclinada invertida en el ejemplo,
# no la escriba en el valor que proporcione.
KAK_FILTER_VALUE.LG1=linux-group1
```

Parámetros de configuración para el Agente de Azure Compute

Los parámetros de configuración para el Agente de Azure Compute se visualizan en tablas que los agrupan por secciones.

1. Tabla 16 en la página 218: Credenciales necesarias para acceder a la suscripción de Azure que contiene los recursos de Azure Compute que se han de supervisar.
2. Tabla 17 en la página 219: Cree los subnodos de agente para definir agrupaciones de máquinas virtuales. Cada nombre de subnodo debe ser exclusivo en el entorno. Se sugiere no tener más de 50 máquinas virtuales por subnodo.

Tabla 16. Credenciales de suscripción de Azure

Nombre de parámetro	Descripción	Nombre de parámetro del archivo de configuración silenciosa
ID de suscripción	El ID asignado por Azure para la suscripción que se supervisa.	**KAK_SUBSCRIPTION_ID**
ID de arrendatario	El ID del arrendatario que ha asignado Azure. Se utiliza para iniciar sesión en la API de servicio de Azure.	**KAK_TENANT_ID**
ID de cliente	El ID de cliente que ha asignado Azure para identificar este agente como aplicación externa que supervisa los servicios de cálculo de Azure.	**KAK_CLIENT_ID**
Clave secreta o contraseña	La clave de acceso secreta o contraseña que ha creado Azure para la aplicación cliente. **Importante:** Windows Si la **Clave secreta o contraseña** contiene un signo igual (=), debe escribirla de nuevo cada vez que vuelva a configurar el agente.	**KAK_SECRET_PASSWORD**

Tabla 17. Subnodo de máquina virtual de Azure Compute

Nombre de parámetro	**Descripción**	**Nombre de parámetro del archivo de configuración silenciosa**
Nombre de subnodo	El nombre del subnodo de Azure Compute para la recopilación de datos. Por ejemplo, *azc1*. El nombre del subnodo debe ser exclusivo en el entorno. Este alias forma parte del nombre de sistema gestionado (MSN) y se utiliza para identificar visualmente el entorno supervisado en la Consola de Cloud APM. **Nota:** Este alias puede ser cualquier cosa que elija para representar la instancia del subnodo de Azure Compute con las restricciones siguientes. Se pueden utilizar letras del alfabeto latino (a-z, A-Z), números arábigos (0-9), el carácter de guión o signo menos (-) y el carácter de subrayado (_) para crear nombres de instancia de subnodo de agente. La longitud máxima de un nombre de subnodo de Azure Compute es de 25 caracteres.	Cada uno de los parámetros siguientes debe utilizar un punto (.) seguido de un agente **Nombre de subnodo** como sufijo. El **Nombre de subnodo** debe ser el mismo para cada parámetro de subnodo. Las instancias de subnodo de agente nuevas deben utilizar un **Nombre de subnodo** exclusivo para su conjunto de parámetros. Por ejemplo, una instancia de subnodo de agente puede utilizar *.azc1* y otra instancia de subnodo de agente puede utilizar *.azc2* en lugar de *.nombre_subnodo* en los nombres de parámetro siguientes.
Tipo de filtro	El tipo de filtro que se debe aplicar.	**KAK_FILTER_TYPE.nombre_subnodo** Valores válidos, **TODOS** Todos **TAG_NAME_VALUE** Par de etiqueta nombre-valor **RESOURCE_GROUP** Grupo de recursos

Tabla 17. Subnodo de máquina virtual de Azure Compute (continuación)		
Nombre de parámetro	**Descripción**	**Nombre de parámetro del archivo de configuración silenciosa**
Valor de filtro	El valor de filtro correspondiente al **Tipo de filtro** seleccionado. Este valor puede ser un **Grupo de recursos** o **Par de etiqueta nombre-valor**. Déjelo vacío para el **Tipo de filtro Todos**. Para la configuración de línea de mandatos, puede que aparezca una barra inclinada invertida en el ejemplo. No escriba ninguna barra inclinada invertida en el valor que proporcione. Ejemplos de los pares tipo de filtro y valor de filtro: • Subnodo de Azure Compute para supervisar todas las máquinas virtuales. Deje el valor del filtro vacío. El valor del filtro no se necesita y se omite en el tipo de filtro **Todos**. – Tipo de filtro: **Todos** – Valor de filtro: • Subnodo de Azure Compute para supervisar todas las máquinas virtuales con un nombre de etiqueta de DTAP y un valor de etiqueta que coincide con la serie `prod`. – Tipo de filtro: **Par de etiqueta nombre-valor** – Valor de filtro: `DTAP:prod` • Subnodo de Azure Compute para supervisar todas las máquinas virtuales con una propiedad de grupo de recursos que coincide con la serie `linux-group1`. – Tipo de filtro: **Grupo de recursos** – Valor de filtro: `linux-group1`	**KAK_FILTER_VALUE.nombre_subnodo**

Configuración de la supervisión de Cassandra

Debe configurar Agente de Cassandra de modo que el agente pueda recopilar datos de los nodos del clúster para supervisar el estado de la base de datos Cassandra.

Antes de empezar

Revise los requisitos previos de hardware y software, consulte Software Product Compatibility Reports para el agente de Cassandra

Acerca de esta tarea

El Agente de Cassandra es un agente de múltiple instancia. Deberá crear la primera instancia e iniciar el agente manualmente.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

- Para configurar el agente en sistemas Windows, puede utilizar la ventana IBM Cloud Application Performance Management o el archivo de respuestas silencioso.
- Para configurar el agente en sistemas Linux puede ejecutar el script y responder a las solicitudes, o utilizar el archivo de respuestas silencioso.

Configuración del agente en sistemas Windows

Puede utilizar la ventana de IBM Cloud Application Performance Management para configurar el agente en sistemas Windows.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Plantilla** en la columna **Tarea/Subsistema** y pulse **Configurar utilizando los valores predeterminados**.

   Se abrirá la ventana **Monitoring Agent for Cassandra**.
3. En el campo **Especificar un nombre de instancia exclusivo**, escriba el nombre de una instancia del agente y pulse **Aceptar**.
4. En la ventana **Monitoring Agent for Cassandra**, especifique valores para los parámetros de configuración y pulse **Aceptar**.

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 223.
5. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón la instancia de agente que ha creado y pulse **Iniciar**.

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información acerca de cómo usar la consola, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente en sistemas Linux

Para configurar el agente en sistemas operativos Linux, debe ejecutar el script y responder a las solicitudes.

Procedimiento

1. En la línea de mandatos, cambie la vía de acceso al directorio de instalación de agente.
   Ejemplo: `/opt/ibm/apm/agent/bin`
2. Ejecute el mandato siguiente, donde nombre_instancia es el nombre que asignará a la instancia:
   `./cassandra-agent.sh config` *`nombre_instancia`*
3. Cuando la línea de mandatos muestre el siguiente mensaje, escriba 1 y especifique:

   ```
   Edit 'Monitoring Agent for Cassandra' setting? [1=Yes, 2=No]
   ```
4. Especifique valores para los parámetros de configuración cuando se le solicite.

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 223.
5. Ejecute el mandato siguiente para iniciar el agente:

```
./cassandra-agent.sh start nombre_instancia
```

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea
Puede utilizar el archivo de respuestas silencioso para configurar el Agente de Cassandra en sistemas Linux y Windows. Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

1. En un editor de texto, abra el archivo de configuración silencioso que está disponible en la siguiente ubicación y especifique valores para todos los parámetros:

   Windows `dir_instalación\samples\cassandra_silent_config_windows.txt`
   Linux `dir_instalación\samples\cassandra_silent_config_UNIX.txt`

   Windows `C:\IBM\APM\samples`

   Linux `/opt/ibm/apm/agent/samples`

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 223.
2. En la línea de mandatos, cambie la vía de acceso a `dir_instalación\bin`.
3. Ejecute el mandato siguiente:

   Windows `cassandra-agent.bat config nombre_instancia dir_instalación \samples\cassandra_silent_config_windows.txt`
   Linux `cassandra-agent.sh config nombre_instancia dir_instalación\samples \cassandra_silent_config_UNIX.txt`
4. Inicie el agente.

   Windows En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón la instancia de agente que ha creado y pulse **Iniciar**.
   Linux Ejecute el mandato siguiente `./cassandra-agent.sh start nombre_instancia`

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Parámetros de configuración del agente

Al configurar el Agente de Cassandra, puede cambiar el valor predeterminado de los parámetros, como por ejemplo Dirección IP y JMX_PORT.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del Agente de Cassandra.

Tabla 18. Nombres y descripciones de los parámetros de configuración

Nombre de parámetro	Descripción	Campo obligatorio
Nombre de instancia	El valor predeterminado para este campo es igual que el valor que se especifica en el campo **Especificar un nombre de instancia exclusivo**.	Sí
Dirección IP	La dirección IP de cualquier nodo del clúster.	Sí
JMX_PORT	El número de puerto JMX para habilitar la supervisión. **Importante:** asegúrese de especificar el puerto JMX, el nombre de usuario JMX y la contraseña de JMX en todo el clúster. Si el nodo a través del cual el agente está conectado al clúster no funciona, el agente puede recopilar datos a través de un nodo diferente en el clúster mediante los mismos parámetros.	Sí
Nombre de usuario_JMX	El nombre de usuario para acceder a JMX.	No
Contraseña_JMX	La contraseña para acceder a JMX.	No

Configuración de la supervisión de Cisco UCS

El Monitoring Agent for Cisco UCS supervisa la Infraestructura virtual de Cisco UCS mediante la conexión a Cisco UCSM. Debe configurar el Agente de Cisco UCS para que el agente pueda recopilar los datos de Cisco UCS.

Antes de empezar

- Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Cisco UCS.
- Asegúrese de que el usuario, que se conecta a la infraestructura UCSM de Cisco, tiene privilegios de administrador o aaa. Utilice un ID de usuario existente, que tenga privilegios de administrador o aaa, o cree un ID de usuario nuevo.
- Si el Agente de Cisco UCS se ha configurado para comunicarse con sus orígenes de datos de Cisco UCS que utilizan el agente SSL, añada el certificado SSL de cada origen de datos al almacén de confianza del certificado del agente. Para obtener más información sobre cómo habilitar la comunicación SSL con orígenes de datos de Cisco UCS, consulte “Habilitación de la comunicación SSL con orígenes de datos de Cisco UCS” en la página 228.

Acerca de esta tarea

El Agente de Cisco UCS es un agente de múltiple instancia. Deberá crear la primera instancia e iniciar el agente manualmente.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Versión de agente. Para acceder a la documentación de los releases anteriores del agente, consulte la tabla siguiente:

Tabla 19. Versiones de agente y documentación	
Versión de Agente de Cisco UCS	**Documentación**
7.2.0.4, 7.2.0.3	IBM Cloud Application Performance Management **Nota:** El enlace abre un tema del Knowledge Center en local.
7.2.0.2	IBM Performance Management 8.1.3 **Nota:** El enlace abre un tema del Knowledge Center en local.
7.2.0.1	IBM Performance Management 8.1.2 **Nota:** El enlace abre un tema del Knowledge Center en local.

Los atributos de configuración definen qué infraestructura de Cisco UCS se supervisa. Los atributos definen una conexión a Cisco UCSM 1.4 o posterior. Puede configurar más de una instancia del agente de supervisión en un host de supervisión remoto. Puede crear también instancias individuales para supervisar la infraestructura de Cisco UCS específica.

Una vez se ha instalado el Agente de Cisco UCS, puede iniciar el agente. Sin embargo, debe configurar manualmente el agente para ver datos de todos los atributos de agente.

- Para configurar el agente en sistemas Windows, puede utilizar la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
- Para configurar el agente en sistemas Linux puede ejecutar el script y responder a las solicitudes, o utilizar el archivo de respuestas silencioso.

Configuración del agente en sistemas Windows

Puede configurar el agente en sistemas operativos Windows mediante la ventana **IBM Performance Management**. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Acerca de esta tarea

El Agente de Cisco UCS proporciona valores predeterminados para algunos parámetros. Puede especificar diferentes valores para estos parámetros.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Monitoring Agent for Cisco UCS** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar el agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar el agente de nuevo, pulse **Reconfigurar**.
3. En la ventana Monitoring Agent for Cisco UCS, realice los pasos siguientes:
   a) Escriba un nombre exclusivo para la instancia del Agente de Cisco UCS y pulse **Aceptar**.
   b) En la pestaña **CONFIG**, especifique valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.
   c) En la pestaña **LOG_CONFIG**, especifique valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.

   Para obtener información sobre los parámetros de configuración de cada pestaña de la ventana Monitoring Agent for Cisco UCS, consulte los temas siguientes:

- "Parámetros de configuración del agente" en la página 227
- "Parámetros de configuración del proveedor de datos" en la página 228

4. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Monitoring Agent for Cisco UCS** y luego pulse **Iniciar**.

Qué hacer a continuación

- Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

  Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.
- Si está supervisando un entorno Cisco UCS de gran tamaño, es posible que sea necesario aumentar el tamaño de almacenamiento dinámico para el proveedor de datos Java™. Para obtener más información, consulte "Aumento del tamaño de almacenamiento dinámico de Java" en la página 229.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

- Para configurar el Agente de Cisco UCS en modalidad silenciosa, realice los pasos siguientes:
  a) En un editor de texto, abra el archivo `cisco_ucs_silent_config.txt` que está disponible en la siguiente vía de acceso:
     – Linux *dir_instalación*`/samples/cisco_ucs_silent_config.txt`

       Ejemplo: `/opt/ibm/apm/agent/samples/cisco_ucs_silent_config.txt`
     – Windows *dir_instalación*`\samples\cisco_ucs_silent_config.txt`

       Ejemplo: `C:\IBM\APM\samples\cisco_ucs_silent_config.txt`

  b) En el archivo `cisco_ucs_silent_config.txt`, especifique valores para todos los parámetros obligatorios. También puede modificar los valores predeterminados de otros parámetros.

     Para obtener información sobre los parámetros de configuración, consulte los siguientes temas:
     – "Parámetros de configuración del agente" en la página 227
     – "Parámetros de configuración del proveedor de datos" en la página 228

  c) Guarde y cierre el archivo `cisco_ucs_silent_config.txt` y ejecute el mandato siguiente:
     – Linux *dir_instalación*`/bin/cisco_ucs-agent.sh config` *nombre_instancia* *dir_instalación*`/samples/cisco_ucs_silent_config.txt`

       Ejemplo: **`/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh config nombre_instancia /opt/ibm/apm/agent/samples/cisco_ucs_silent_config.txt`**

– Windows *dir_instalación*\bin\cisco_ucs-agent.bat config *nombre_instancia* *dir_instalación*\samples\cisco_ucs_silent_config.txt

Ejemplo: **C:\IBM\APM\bin\cisco_ucs-agent.bat config nombre_instancia C:\IBM\APM\samples\cisco_ucs_silent_config.txt**

Donde

nombre_instancia
Nombre que desea dar a la instancia.

dir_instalación
Vía de acceso donde está instalado el agente.

Importante: Asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

d) Ejecute el mandato siguiente para iniciar el agente:

– Linux *dir_instalación*/bin/cisco_ucs-agent.sh start *nombre_instancia*

Ejemplo: **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh start nombre_instancia**

– Windows *dir_instalación*\bin\cisco_ucs-agent.bat start *nombre_instancia*

Ejemplo: **C:\IBM\APM\bin\cisco_ucs-agent.bat start nombre_instancia**

Qué hacer a continuación

- Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

  Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.
- Si está supervisando un entorno Cisco UCS de gran tamaño, es posible que sea necesario aumentar el tamaño de almacenamiento dinámico para el proveedor de datos Java™. Para obtener más información, consulte "Aumento del tamaño de almacenamiento dinámico de Java" en la página 229.

Configuración del agente respondiendo a solicitudes

Para configurar el agente en sistemas operativos Linux, debe ejecutar el script y responder a las solicitudes.

Procedimiento

- Para configurar el agente mediante la ejecución del script y las respuestas a las solicitudes, siga estos pasos:

  a) En la línea de mandatos, entre el siguiente mandato:

  dir_instalación/bin/cisco_ucs-agent.sh config *nombre_instancia*

  Ejemplo **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh config nombre_instancia**

  Donde

  nombre_instancia
  Nombre que desea dar a la instancia.

  dir_instalación
  Vía de acceso donde está instalado el agente.

  b) Responda a las solicitudes haciendo referencia a los temas siguientes:

  – "Parámetros de configuración del agente" en la página 227
  – "Parámetros de configuración del proveedor de datos" en la página 228

  c) Ejecute el mandato siguiente para iniciar el agente:

dir_instalación/bin/cisco_ucs-agent.sh start *nombre_instancia*

Ejemplo **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh start nombre_instancia**

Qué hacer a continuación

- Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

  Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.
- Si está supervisando un entorno Cisco UCS de gran tamaño, es posible que sea necesario aumentar el tamaño de almacenamiento dinámico para el proveedor de datos Java™. Para obtener más información, consulte "Aumento del tamaño de almacenamiento dinámico de Java" en la página 229.

Parámetros de configuración del agente

Al configurar el Agente de Cisco UCS, puede cambiar el valor predeterminado de los parámetros, como el nombre de instancia y los certificados de validación SSL.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del Agente de Cisco UCS.

Tabla 20. Nombres y descripciones de los parámetros de configuración del Agente de Cisco UCS

Nombre de parámetro	Descripción	Campo obligatorio
Nombre de instancia	El nombre de la instancia. **Restricción:** El campo **Nombre de instancia** muestra el nombre de la instancia que especifica al configurar el agente por primera vez. Al volver a configurar el agente, no puede cambiar el nombre de instancia del agente.	Sí
URL	El URL del Gestor de Cisco UCS. Para establecer el URL del gestor de Cisco UCS, entre el URL en el formato http://dirección_ip/nuova.	Sí
Nombre de usuario	El nombre de usuario del administrador del gestor de Cisco UCS.	Sí
Contraseña	La contraseña del administrador del gestor de Cisco UCS.	Sí
Confirmar contraseña	La misma contraseña que ha especificado en el campo **Contraseña**.	Sí
Vía de acceso de archivo del almacén de confianza SSL	La vía de acceso de archivo del almacén de confianza de la capa de sockets seguros (SSL). Si desea que el agente valide certificados SSL cuando se utilice SSL para comunicarse por la red, especifique la ubicación donde se encuentra el archivo de almacén de confianza SSL.	Sí

Tabla 20. Nombres y descripciones de los parámetros de configuración del Agente de Cisco UCS (continuación)		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Validar certificados SSL	Un valor booleano que indica si el agente valida certificados SSL cuando el agente utiliza SSL para comunicarse por la red. Establezca el valor en Yes si desea que el agente valide certificados SSL cuando el agente utilice SSL para comunicarse a través de la red. Establezca el valor en No para impedir que el agente valide certificados SSL. **Consejo:** Para obtener más información sobre cómo habilitar la comunicación SSL con orígenes de datos de Cisco UCS, consulte "Habilitación de la comunicación SSL con orígenes de datos de Cisco UCS" en la página 228.	Sí

Parámetros de configuración del proveedor de datos

Al configurar el Agente de Cisco UCS, puede cambiar los valores predeterminados de los parámetros del proveedor de datos, por ejemplo el número máximo de archivos de registro del proveedor de datos, el tamaño máximo del archivo de registro y el nivel de detalle que se incluye en el archivo de registro.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del proveedor de datos.

Tabla 21. Nombres y descripciones de los parámetros de configuración del proveedor de datos		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Número máximo de archivos de registro del proveedor de datos	El número máximo de archivos de registro que el proveedor de datos crea antes de grabar encima de los archivos de registro anteriores. El valor predeterminado es 10.	Sí
Tamaño máximo en KB de cada archivo de registro del proveedor de datos	El tamaño máximo en KB que debe alcanzar un archivo de registro del proveedor de datos antes de que el proveedor de datos cree un archivo de registro nuevo. El valor predeterminado es 5190 KB.	Sí
Nivel de detalle en el archivo de registro del proveedor de datos	El nivel de detalle que puede incluirse en el archivo de registro que crea el proveedor de datos. El valor predeterminado es INFO. Los valores válidos son OFF, SEVERE, WARNING, INFO, FINE, FINER, FINEST y ALL.	Sí

Habilitación de la comunicación SSL con orígenes de datos de Cisco UCS

El Agente de Cisco UCS puede configurarse para que se comunique con sus orígenes de datos de Cisco UCS de forma segura utilizando SSL. En esta configuración, debe añadir un certificado de SSL de origen de datos al almacén de confianza del certificado del agente.

Acerca de esta tarea

Importante: La siguiente información sólo se aplica si el agente se configura para validar certificados SSL.

Si la validación de certificados SSL está desactivada, el Agente de Cisco UCS se conecta a orígenes de datos de Cisco UCS, incluso si sus certificados SSL están caducados, no son de confianza o no son válidos. Sin embargo, al desactivar la validación de certificados SSL, la seguridad podría comprometerse, por lo que esta operación debe hacerse con precaución.

Si un origen de datos de Cisco UCS utiliza un certificado SSL que está firmado por una entidad emisora de certificados común (por ejemplo, Verisign, Entrust, o Thawte), no es necesario añadir certificados al almacén de certificados del Agente de Cisco UCS. Sin embargo, si el origen de datos utiliza un certificado que no esté firmado por una entidad emisora de certificados, que es lo que sucede de forma predeterminada, el certificado debe añadirse al almacén de confianza para permitir que el agente se conecte y recopile datos satisfactoriamente .

Procedimiento

1. Copie el archivo de certificados del origen de datos al sistema del agente.
2. Coloque el archivo de certificados en un directorio de su elección en el sistema del agente. No sobrescriba los archivos de certificados. Utilice una etiqueta y nombre de archivo exclusivos para cada certificado que añada.
3. Utilice el mandato `keytool` para añadir un certificado de origen de datos al almacén de confianza de certificados del agente:

```
keytool -import -noprompt -trustcacerts -alias AliasCertificado -file
ArchivoCertificado -keystore AlmacénConfianza -storepass
ContraseñaAlmacénConfianza
```

Donde

AliasCertificado

Se añade una referencia exclusiva para cada certificado al almacén de confianza del agente. Por ejemplo, un alias adecuado para el certificado de *origendatos.ejemplo.com* sería *origendatos*.

ArchivoCertificado

Vía de acceso completa y el nombre de archivo para el certificado de origen de datos de Cisco UCS que se va a añadir al almacén de confianza.

Almacén de confianza

Nombre de archivo y vía de acceso completos a la base de datos de certificados del Agente de Cisco UCS. Utilice la siguiente vía de acceso y nombre de archivo:

- Windows (64 bits) *dir_instalación*`\tmaitm6_x64\kv6.truststore`
- Linux (64 bits) `dir_instalación/lx8266/vm/etc/kv6.truststore`

ContraseñaAlmacénConfianza

ITMFORVE es la contraseña predeterminada para el almacén de confianza del Agente de Cisco UCS. Para cambiar la contraseña, consulte la documentación de Java Runtime a fin de obtener información sobre las herramientas que deben utilizarse.

Importante: Para poder utilizar el mandato `keytool`, debe constar el directorio bin de Java Runtime en la vía de acceso. Utilice los mandatos siguientes:

- Windows (64 bits) `set PATH=%PATH%;dir_instalación\java\java70_x64\jre\bin`
- Linux (64 bits) `PATH="$PATH":/opt/ibm/apm/agent/JRE/lx8266/bin`

4. Después de añadir todos los certificados de origen de datos, inicie el agente de supervisión.

Aumento del tamaño de almacenamiento dinámico de Java

Después de configurar el Agente de Cisco UCS, si va a supervisar un gran entorno Cisco UCS, es posible que tenga que aumentar el tamaño de almacenamiento dinámico para el proveedor de datos de Java.

Acerca de esta tarea

El tamaño de almacenamiento dinámico predeterminado para el proveedor de datos Java es de 256 megabytes. En grandes entornos Cisco UCS, si surge el problema siguiente, es posible que tenga que aumentar el tamaño de almacenamiento dinámico si:

- El proveedor de datos de Java se detiene debido a un problema de `javacore` y crea un archivo denominado `javacore.`*`fecha.hora.número`*`.txt` en el directorio `CANDLEHOME\tmaitm6_x64`.
- El archivo `javacore.`*`fecha.hora.número`*`.txt` contiene la serie `java/lang/OutOfMemoryError`.

Procedimiento

- Windows

  Complete los pasos siguientes para establecer un valor de 1 GB como tamaño de almacenamiento dinámico:

  1. Abra el archivo `%CANDLE_HOME%\TMAITM6_x64\kv6_data_provider.bat`.
  2. Añada la siguiente línea antes de la línea que empieza por `KV6_JVM_ARGS="$KV6_CUSTOM_JVM_ARGS...`:

     ```
     SET KV6_CUSTOM_JVM_ARGS=-Xmx1024m
     ```

  3. Reinicie el agente.
- Linux

  Complete los pasos siguientes para establecer un valor de 1 GB como tamaño de almacenamiento dinámico:

  1. Abra el archivo `$CANDLEHOME/lx8266/vm/bin/kv6_data_provider.sh`.
  2. Añada la siguiente línea antes de la línea que empieza por `KV6_JVM_ARGS="$KV6_CUSTOM_JVM_ARGS...`:

     ```
     KV6_CUSTOM_JVM_ARGS=-Xmx1024m
     ```

  3. Reinicie el agente.

Configuración de la supervisión de Citrix Virtual Desktop Infrastructure

El Agente de Citrix VDI proporciona un punto central de supervisión para recursos Citrix XenDesktop o XenApp, incluidos los grupos de distribución, catálogos, aplicaciones, sistemas de sobremesa, usuarios y sesiones. Antes de que se pueda utilizar el agente, debe configurarlo para recopilar datos a través del controlador de entrega.

Antes de empezar

- Las instrucciones siguientes son para el release más reciente del agente, a excepción de lo indicado.
- Asegúrese de que los requisitos del sistema del Agente de Citrix VDI se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Citrix VDI.
- Asegúrese de que la siguiente información está disponible:
  - Nombre de host del controlador de entrega al que tiene previsto conectarse.
  - Nombre de usuario, contraseña y dominio de OData.
  - Nombre de usuario de PowerShell, contraseña, dominio, puerto de PowerShell, tipo de verificación de SSL y mecanismo de autenticación si habilita la recuperación de suceso de registro de sucesos de Windows y métrica de PowerShell.
- Asegúrese de que la cuenta de usuario operador de agente tenga como mínimo privilegios de administrador de sólo lectura de Citrix. Consulte Habilitación de privilegios de administrador de sólo lectura de Citrix.
- A partir de Agente de Citrix VDI versión 8.1.3.1, la capacidad de recuperar sucesos del registro de sucesos de Windows pasó a estar disponible. Para poder recuperar sucesos del registro de sucesos de Windows de todas las máquinas Desktop Delivery Controller (DDC) y Virtual Delivery Agent (VDA), es necesario habilitar el acceso de PowerShell remoto para la cuenta de usuario especificada durante la

configuración de instancia del agente. Siga estos pasos para asegurarse de que el agente pueda realizar esta función:

1. Inicie la sesión en un sistema Windows como el usuario especificado en la configuración de instancia de agente.
2. Ejecute el siguiente mandato PowerShell, donde *vda_system* es el nombre de una máquina VDA que está encendida:
   ```
   Get-WinEvent -FilterHashtable
   @{ProviderName='Citrix*';LogName='Citrix*';StartTime=((Get-
   Date).AddDays(-10))} -ComputerName vda_system
   ```

- Asegúrese de que las siguientes políticas de equilibrio de carga están habilitadas para el entorno supervisado:
  - Uso de CPU
  - Uso de disco
  - Uso de memoria

  Estas políticas pueden configurarse a través de la aplicación Citrix Studio.

Acerca de esta tarea

El Agente de Citrix VDI es un agente de múltiple instancia. Debe crear como mínimo una instancia e iniciar manualmente la instancia de agente.

La configuración para los servidores XenApp es la misma que para los servidores XenDesktop. Si un nombre o una descripción de parámetro de configuración menciona solo "XenDesktop", también es para XenApp.

Procedimiento

1. Configure el agente en sistemas Windows mediante la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
   - “Configuración del agente en sistemas Windows” en la página 232.
   - “Configuración del agente mediante el archivo de respuestas silencioso” en la página 236.
2. Configure el agente en sistemas Linux con el script que solicita respuestas o el archivo de respuestas silencioso.
   - “Configuración del agente respondiendo a solicitudes” en la página 235.
   - “Configuración del agente mediante el archivo de respuestas silencioso” en la página 236.

Qué hacer a continuación

En la Consola de Cloud APM, vaya al Panel de instrumentos del rendimiento de aplicaciones para ver los datos que se han recopilado. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte “Inicio de la Consola de Cloud APM” en la página 1009.

Si no puede ver los datos en los paneles de instrumentos del agente, consulte primero los registros de conexión del servidor y, a continuación, los registros del proveedor de datos. Las vías de acceso a estos registros se listan aquí:

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Si desea recibir ayuda con la resolución de problemas, consulte el Foro de Cloud Application Performance Management.

Habilitación de privilegios de administrador de sólo lectura de Citrix

Agente de Citrix VDI requiere que la cuenta de usuario de operador de agente tenga como mínimo privilegios de administrador de sólo lectura de Citrix.

Acerca de esta tarea

Para ejecutar estos pasos de forma remota desde un sistema con el complemento de PowerShell de administración delegada de Citrix instalado, utilice el parámetro `AdminAddress`. Por ejemplo, el mandato en el paso 2 se convierte en `New-AdminAdministrator -Name "YOURDOMAIN\NewAdmin" -AdminAddress "controller1.YOURDOMAIN.com"`. Donde *YOURDOMAIN* es el nombre del dominio de red, *NewAdmin* es la cuenta de usuario a la que se proporcionan privilegios de administración de Citrix, y *controller1.YOURDOMAIN.com* es el nombre de dominio completo del servidor del sitio Citrix.

Procedimiento

1. Inicie una sesión de PowerShell con una cuenta de administrador existente de Citrix.
2. Cargue el complemento de PowerShell de administración delegada para gestionar el sitio XenApp o XenDesktop de Citrix.

   `(Add-PSSnapin Citrix.DelegatedAdmin.Admin.V1)`
3. Añada la cuenta de usuario del operador del agente como administrador del sitio Citrix.

   `New-AdminAdministrator -Name "YOURDOMAIN\NewAdmin"`

   Donde *YOURDOMAIN* es el nombre del dominio de red y *NewAdmin* es la cuenta de usuario a la que se proporcionan privilegios de administración de Citrix.
4. Busque si hay roles y ámbitos disponibles para asignar a *NewAdmin*.

   ```
   Get-AdminRole
   Get-AdminScope
   ```
5. Asigne roles a la cuenta de usuario del operador de agente, incluidos los permisos de administración de sólo lectura.

   `Add-AdminRight -Administrator "YOURDOMAIN\NewAdmin" -Role "Read Only Administrator" -Scope "All"`

   Donde

   - *YOURDOMAIN* es el nombre del dominio de red.
   - *NewAdmin* es la cuenta de usuario a la que se proporcionan privilegios de administración de Citrix.
   - *Read Only Administrator* es el rol de administrador del sitio Citrix que está asignando.
   - *All* es el ámbito del administrador del sitio Citrix que está asignando.
6. Confirme la adición y los cambios del administrador.

   `Get-AdminAdministrator -Name "YOURDOMAIN\NewAdmin"`

   Donde *YOURDOMAIN* es el nombre del dominio de red y *NewAdmin* es la cuenta de usuario a la que se proporcionan privilegios de administración de Citrix.

Configuración del agente en sistemas Windows

Puede configurar el Agente de Citrix VDI en sistemas operativos Windows utilizando la ventana de IBM Cloud Application Performance Management. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.

2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la plantilla **Monitoring Agent for Citrix Virtual Desktop Infrastructure** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar una instancia de agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar la instancia de agente de nuevo, púlsela con el botón derecho del ratón y luego pulse **Reconfigurar**.
3. Especifique un nombre de instancia exclusivo y luego pulse **Aceptar**. Utilice solamente letras, números, el carácter de subrayado y el carácter menos en el nombre de la instancia. Por ejemplo, `vdi_inst2`.

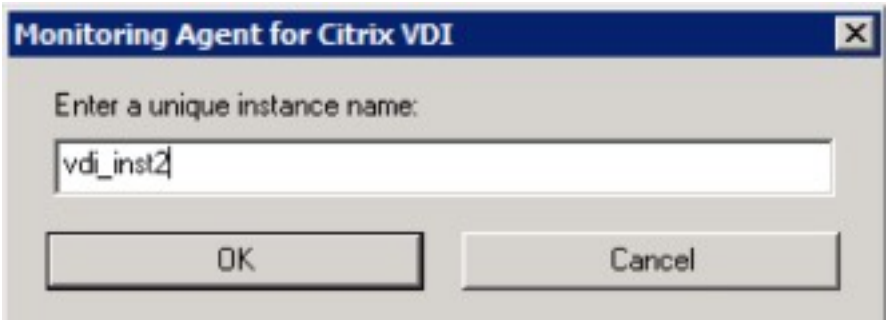


Figura 13. La ventana para especificar un nombre de instancia exclusivo.

4. Pulse **Siguiente** en la ventana de nombre de instancia de agente.

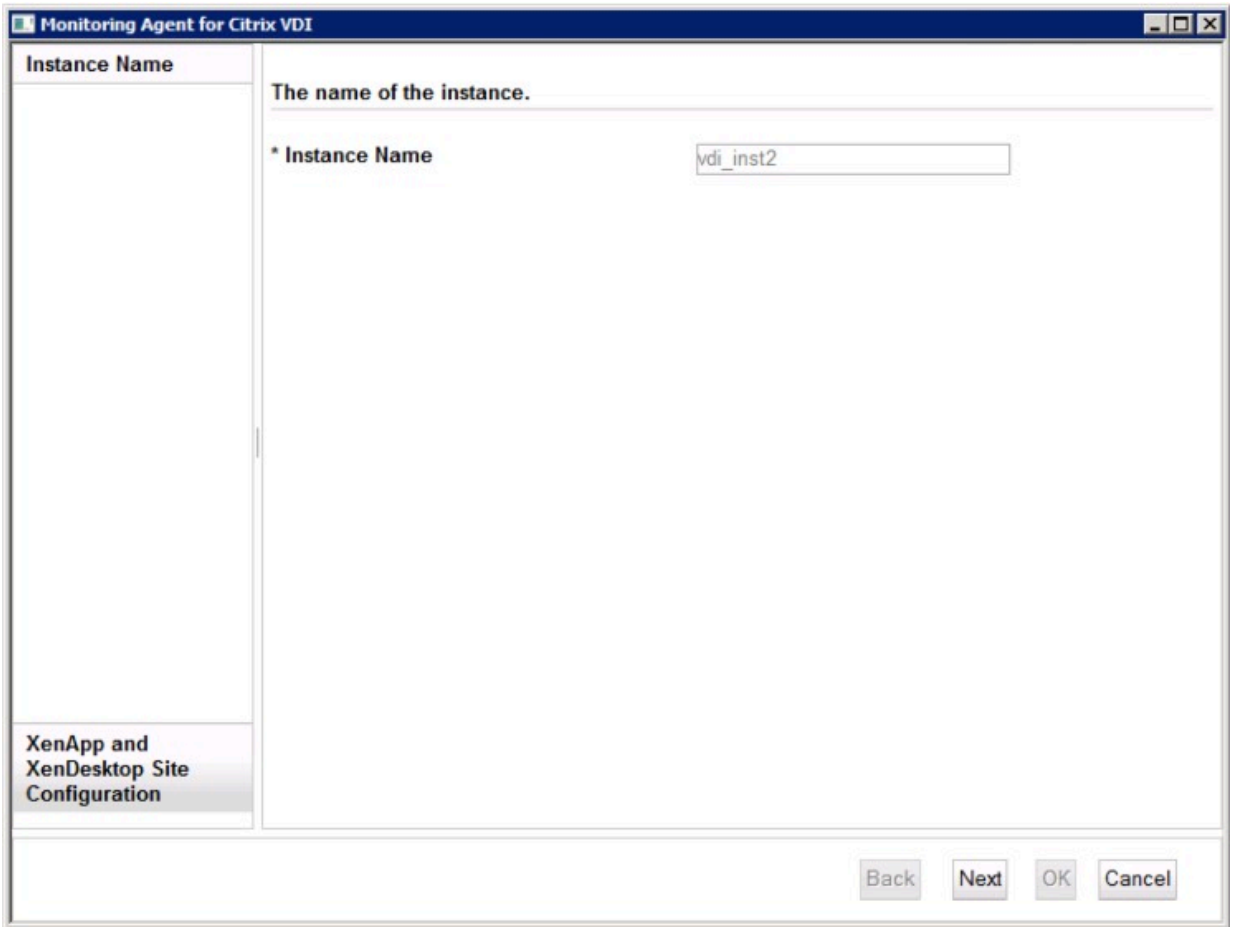


Figura 14. La ventana de nombre de instancia de agente.

5. Especifique los valores de plantilla de instancia de **Configuración del sitio XenApp y XenDesktop**.

   Nota: Esta sección no es la configuración de instancia del sitio XenApp o XenDesktop. Es una selección de plantilla para establecer lo que se utiliza en los valores predeterminados cuando añade las configuraciones de instancia del sitio XenApp o XenDesktop reales en el paso 6.

Consulte la sección Tabla 22 en la página 238 para obtener una descripción de cada uno de los parámetros de configuración.

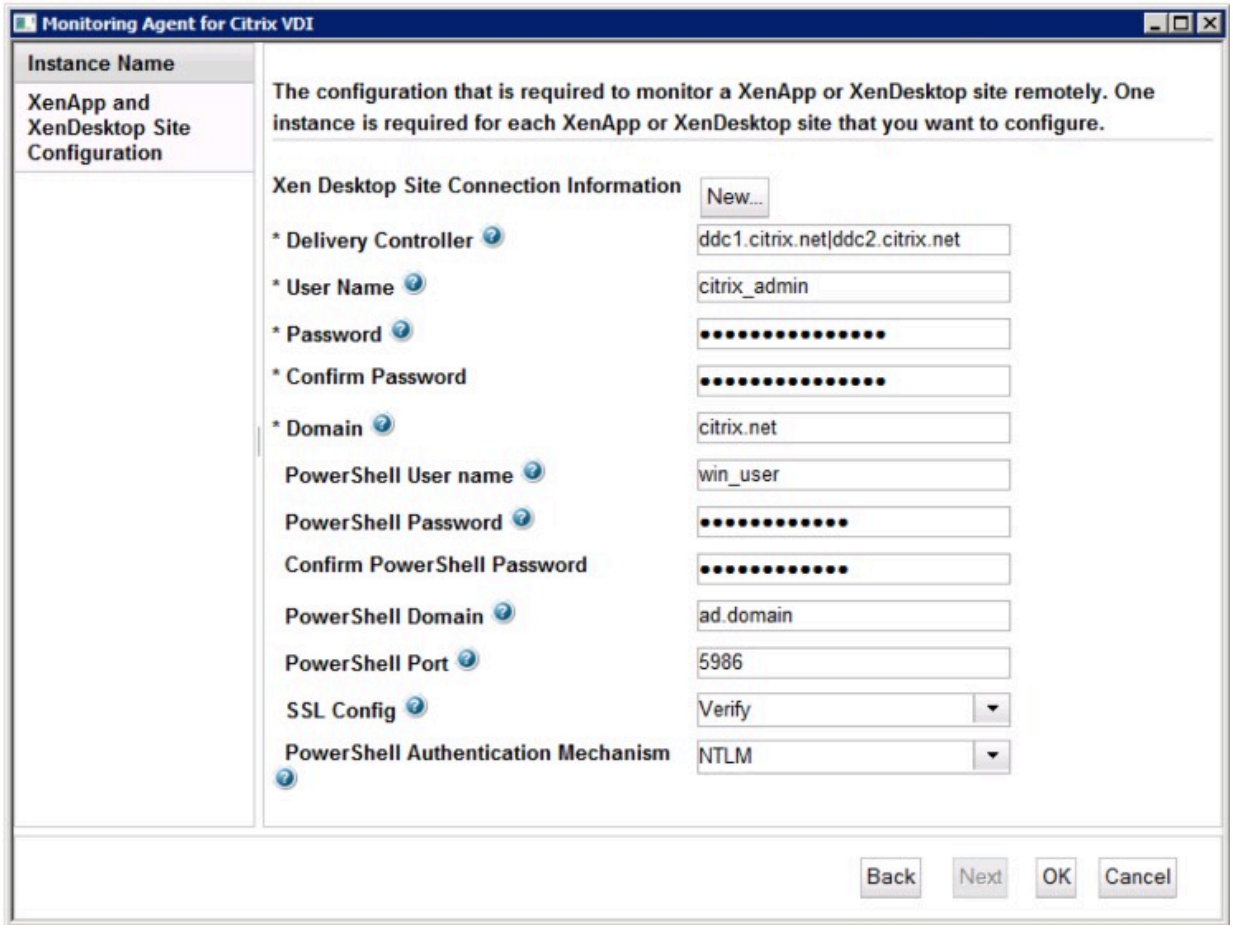


Figura 15. La ventana para especificar valores de plantilla de instancia del sitio XenApp o XenDesktop.

6. Pulse **Nuevo** y especifique los valores de instancia del sitio XenApp o XenDesktop y a continuación pulse **Siguiente**.

   Consulte la sección Tabla 22 en la página 238 para obtener una descripción de cada uno de los parámetros de configuración.

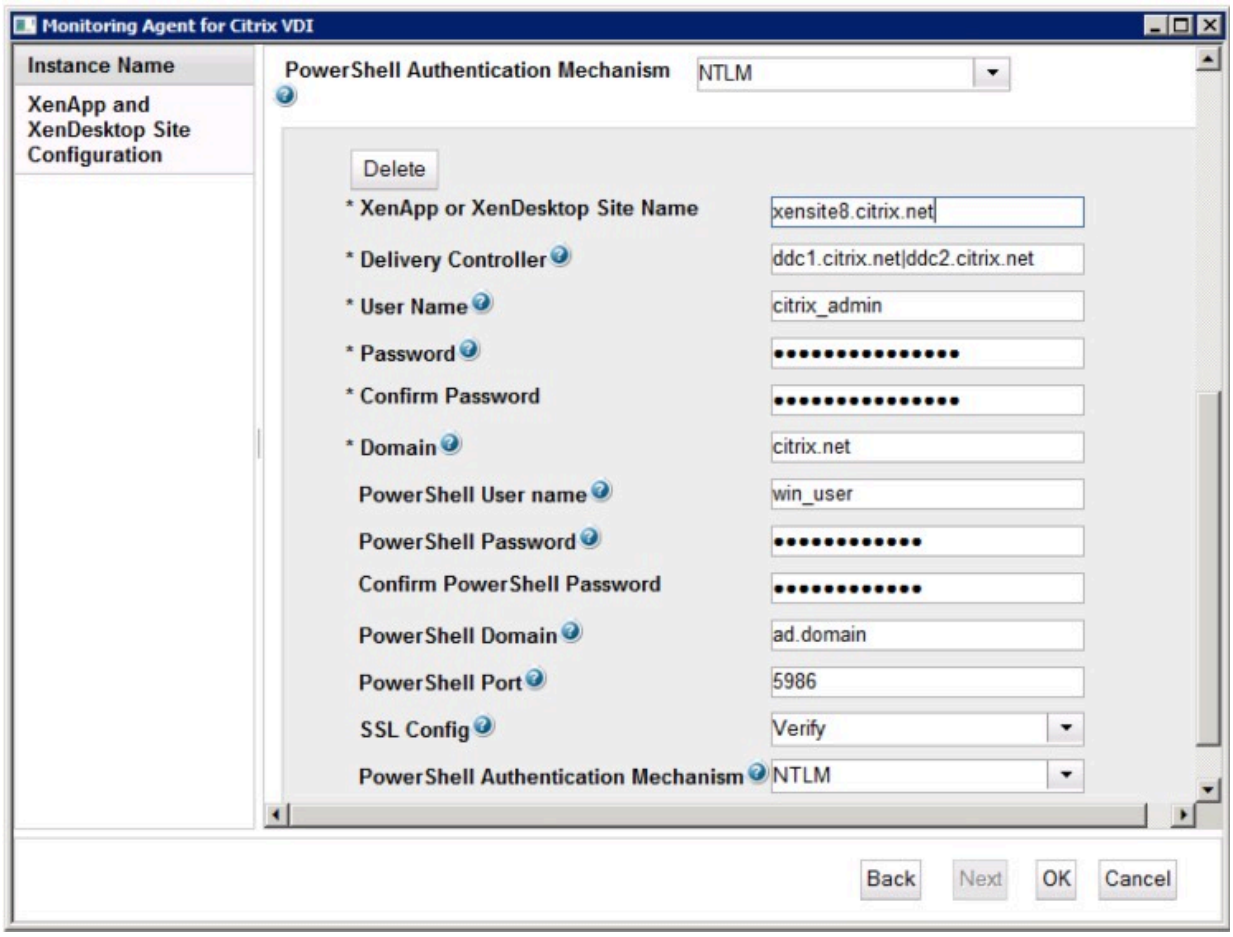


Figura 16. La ventana para especificar los valores de instancia del sitio XenApp o XenDesktop.

Nota: El parámetro **`Nombre de usuario de PowerShell`** y todos los parámetros de PowerShell siguientes solo son necesarios en la "Habilitación de la supervisión de sucesos de Windows y métricas de PowerShell" en la página 239. Estas variables de entorno avanzadas están desactivadas de forma predeterminada debido a la carga significativa que ponen sobre el sistema supervisado.

Nota: Asegúrese de que los parámetros **`Configuración SSL`** y **`Mecanismo de autenticación de PowerShell`** se establecen correctamente para cada instancia de sitio XenApp o XenDesktop nueva. Un defecto hace que se establezcan los valores predeterminados en lugar de los valores de plantilla.

7. Pulse **Aceptar** para completar la configuración.
8. En la ventana de IBM Cloud Application Performance Management, pulse con el botón derecho del ratón la instancia que ha configurado y luego pulse **Iniciar**.

Configuración del agente respondiendo a solicitudes

Después de la instalación del Agente de Citrix VDI, debe configurarlo para poder iniciar el agente. Si el Agente de Citrix VDI está instalado en una máquina Linux local, puede seguir estas instrucciones para configurarlo interactivamente a través de solicitudes de línea de mandatos.

Acerca de esta tarea

Recuerde: Si está volviendo a configurar una instancia de agente configurada, se visualiza el valor que se establece en la última configuración para cada opción. Si desea borrar un valor existente, pulse la tecla de espacio cuando se visualice el valor.

Procedimiento

Siga estos pasos para configurar el Agente de Citrix VDI ejecutando un script y respondiendo a solicitudes.

1. Ejecute el mandato siguiente:

   ```
   dir_instalación/bin/citrixvdi-agent.sh
   config nombre_instancia
   ```

   donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/citrixvdi-agent.sh config vdi_inst01
   ```

2. Responda a las solicitudes para establecer valores de configuración para el agente.

   Consulte la sección "Parámetros de configuración para el Agente de Citrix VDI" en la página 237 para obtener una descripción de cada uno de los parámetros de configuración.

   Nota: El parámetro **Nombre de usuario de PowerShell** y todos los parámetros de PowerShell siguientes solo son necesarios en la "Habilitación de la supervisión de sucesos de Windows y métricas de PowerShell" en la página 239. Estas variables de entorno avanzadas están desactivadas de forma predeterminada debido a la carga significativa que ponen sobre el sistema supervisado.

3. Ejecute el mandato siguiente para iniciar el agente:

   ```
   dir_instalación/bin/citrixvdi-agent.sh
   start nombre_instancia
   ```

   Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/citrixvdi-agent.sh start vdi_inst01
   ```

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

- Configure el Agente de Citrix VDI en modalidad silenciosa:
  a) En un editor de texto, abra el archivo `citrixvdi_silent_config.txt` en una de las vías de acceso siguientes.
     - Linux *dir_instalación*`/samples/citrixvdi_silent_config.txt`

       Por ejemplo, `/opt/ibm/apm/agent/samples/citrixvdi_silent_config.txt`
     - Windows *dir_instalación*`\samples\citrixvdi_silent_config.txt`

Por ejemplo, `C:\IBM\APM\samples\citrixvdi_silent_config.txt`

Donde *dir_instalación* es la vía de acceso donde está instalado el agente.

b) En el archivo `citrixvdi_silent_config.txt` especifique valores para todos los parámetros obligatorios y modifique los valores predeterminados de otros parámetros según sea necesario.

Consulte la sección "Parámetros de configuración para el Agente de Citrix VDI" en la página 237 para obtener una descripción de cada uno de los parámetros de configuración.

Nota: El parámetro **Nombre de usuario de PowerShell** y todos los parámetros de PowerShell siguientes solo son necesarios en la "Habilitación de la supervisión de sucesos de Windows y métricas de PowerShell" en la página 239. Estas variables de entorno avanzadas están desactivadas de forma predeterminada debido a la carga significativa que ponen sobre el sistema supervisado.

c) Guarde y cierre el archivo `citrixvdi_silent_config.txt` y ejecute el mandato siguiente:

- Linux *dir_instalación*`/bin/citrixvdi-agent.sh config` **nombre_instancia** *dir_instalación*`/samples/citrixvdi_silent_config.txt`

  Por ejemplo, **/opt/ibm/apm/agent/bin/citrixvdi-agent.sh config vdi_inst01 /opt/ibm/apm/agent/samples/citrixvdi_silent_config.txt**

- Windows *dir_instalación*`\bin\citrixvdi-agent.bat config` **nombre_instancia** *dir_instalación*`\samples\citrixvdi_silent_config.txt`

  Por ejemplo, **C:\IBM\APM\bin\citrixvdi-agent.bat config vdi_inst01 C:\IBM\APM\samples\citrixvdi_silent_config.txt**

Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

Importante: Asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

d) Ejecute el mandato siguiente para iniciar el agente:

- Linux *dir_instalación*`/bin/citrixvdi-agent.sh start` **nombre_instancia**

  Por ejemplo, **/opt/ibm/apm/agent/bin/citrixvdi-agent.sh start vdi_inst01**

- Windows *dir_instalación*`\bin\citrixvdi-agent.bat start` **nombre_instancia**

  Por ejemplo, **C:\IBM\APM\bin\citrixvdi-agent.bat start vdi_inst01**

Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

Parámetros de configuración para el Agente de Citrix VDI

Los parámetros de configuración del Agente de Citrix VDI se visualizan en una tabla.

1. Valores del Agente VDI de Citrix VDI - Valores de entorno del Agente VDI de Citrix.

Tabla 22. Valores del Agente VDI de Citrix		
Nombre de parámetro	**Descripción**	**Nombre de parámetro del archivo de configuración silenciosa**
Nombre del sitio XenApp o XenDesktop	Proporcione un nombre para identificar la instancia del agente del sitio XenApp o XenDesktop. Por ejemplo, *vdi_inst2* **Nota:** Este alias puede ser cualquier cosa que elija para representar la instancia del agente del servidor de WebLogic con las restricciones siguientes. Sólo se pueden utilizar letras, números arábigos, el carácter de subrayado y el símbolo "menos" en el nombre de la conexión. La longitud máxima de un nombre de conexión son 25 caracteres.	Cada uno de los parámetros siguientes debe tener un sufijo de nombre de instancia que sea el mismo para cada parámetro de una instancia de agente. Las instancias de agente nuevas deben utilizar un nombre de instancia exclusivo para su conjunto de parámetros. Por ejemplo, una instancia de agente puede utilizar *.vdi1* y otra instancia de agente puede utilizar *.vdi2* en lugar de *.nombre_instancia* en los nombres de parámetro siguientes.
Controlador de entrega	Nombre de host o dirección IP del controlador de entrega. Si hay varios DDCs establecidos en un clúster, se puede proporcionar una lista de controladores de entrega separada por '|'.	**KVD_XDS_DELIVERY_CONTROLLER.nombre_instancia**
Nombre de usuario	Nombre de usuario que se utiliza para autenticar con la API de OData en el controlador de entrega de XenApp o XenDesktop.	**KVD_XDS_ODATA_USERNAME.nombre_instancia**
Contraseña	Contraseña que se utiliza para autenticar con la API de OData en el controlador de entrega de XenApp o XenDesktop.	**KVD_XDS_ODATA_PASSWORD.nombre_instancia**
Dominio	Dominio que se utiliza para autenticar con la API de OData en el controlador de entrega de XenApp o XenDesktop.	**KVD_XDS_ODATA_DOMAIN.nombre_instancia**
Nombre usuario de PowerShell	Nombre de usuario que se utiliza para la autenticación de llamadas de PowerShell con máquinas VDA y DDC remotas. **Nota:** Este y todos los parámetros de PowerShell siguientes solo son necesarios en la "Habilitación de la supervisión de sucesos de Windows y métricas de PowerShell" en la página 239. Estas variables de entorno avanzadas están desactivadas de forma predeterminada debido a la carga significativa que ponen sobre el sistema supervisado.	**KVD_XDS_POWERSHELL_USERNAME.nombre_instancia**
Contraseña de PowerShell	Contraseña asociada al nombre de usuario de PowerShell proporcionado.	**KVD_XDS_POWERSHELL_PASSWORD.nombre_instancia**
Dominio de PowerShell	Dominio asociado al nombre de usuario de PowerShell proporcionado.	**KVD_XDS_POWERSHELL_DOMAIN.nombre_instancia**

Tabla 22. Valores del Agente VDI de Citrix (continuación)		
Nombre de parámetro	**Descripción**	**Nombre de parámetro del archivo de configuración silenciosa**
Puerto de PowerShell	El puerto SSL abierto para que lo utilice WinRm. Los puertos de conexión remota predeterminados de PowerShell son 5985 para HTTP y 5986 para HTTPS.	**KVD_XDS_POWERSHELL_PORT.nombre_instancia**
Requisito SSL	Elija la opción SSL necesaria para su entorno.	**KVD_XDS_SSL_CONFIG.nombre_instancia** Valores válidos, **KVD_XDS_SSL_CONFIG_VERIFY** Verificar **KVD_XDS_SSL_CONFIG_NOVERIFY** No verificar **KVD_XDS_SSL_CONFIG_NOSSL** No SSL
Mecanismo de autenticación de PowerShell	Define el tipo de autenticación utilizado para crear una credencia para recuperar información de sistemas remotos con PowerShell.	**KVD_XDS_POWERSHELL_AUTH_MECH.nom_instancia** Valores válidos, **KVD_XDS_POWERSHELL_BASIC** Básico **KVD_XDS_POWERSHELL_CREDSSP** CredSSP **KVD_XDS_POWERSHELL_NTLM** NTLM **KVD_XDS_POWERSHELL_DEFAULT** Valor predeterminado **KVD_XDS_POWERSHELL_DIGEST** Resumen **KVD_XDS_POWERSHELL_KERBEROS** Kerberos **KVD_XDS_POWERSHELL_NEGOTIATE** Negociar

Habilitación de la supervisión de sucesos de Windows y métricas de PowerShell

Habilitación de la supervisión de sucesos de Windows y métricas de PowerShell con este procedimiento. La supervisión de estos datos puede tener un impacto significativo sobre el rendimiento del sistema supervisado.

Antes de empezar

Asegúrese de que los parámetros de configuración de PowerShell están establecidos.

Acerca de esta tarea

Una o varias de las variables de entorno avanzadas siguientes deben estar habilitadas para que el agente supervise los sucesos de Windows y las métricas de PowerShell.

GET_SESSION_LATENCY
Si la latencia de sesión y el tiempo de ida y vuelta se recuperan de forma remota desde el VDA conectado de PowerShell.

GET_VDA_MACHINE_METRICS_REMOTELY
Si las métricas de máquina VDA se recuperan remotamente de PowerShell.

RETRIEVE_WINDOWS_EVENTS
Si los sucesos de registro de suceso Windows se recuperan de PowerShell de los VDAs y DDCs de Windows.

Procedimiento

1. Vaya al directorio de instalación de agente del Agente de Citrix VDI:
   - Linux *dir_instalación*/config
   - Windows *dir_instalación*\TMAITM6_x64

   Donde *dir_instalación* es la vía de acceso donde está instalado el agente.
2. Edite el archivo de configuración del Agente de Citrix VDI para establecer una o varias de las variables *GET_SESSION_LATENCY*, *GET_VDA_MACHINE_METRICS_REMOTELY* y *RETRIEVE_WINDOWS_EVENTS* en `true`.
   - Linux `vd.environment`
   - Windows KVDENV_*nombre_instancia*

   donde *nombre_instancia* es el nombre de la instancia de agente.
3. Reinicie el agente.

   Importante: Para que estos valores sean valores predeterminados para todas las instancias de agente nuevas, establézcalos en `true` en los archivos de plantilla de configuración:
   - Linux Este valor ya se convierte en el valor predeterminado de las instancias de agente nuevas editando `vd.environment` en el Paso 2.
   - Windows KVDENV

Ejemplo

```
GET_SESSION_LATENCY=true
GET_VDA_MACHINE_METRICS_REMOTELY=true
RETRIEVE_WINDOWS_EVENTS=true
```

Configuración de la supervisión DataPower

Para supervisar dispositivos DataPower, primero debe completar algunas tareas de configuración en sus dispositivos y a continuación configure el Monitoring Agent for DataPower.

Consejo: Pulse APM v8: Configuring DataPower monitoring in IBM APM para ver un vídeo sobre el proceso de configuración básico de la supervisión de DataPower.

Configuración de dispositivos DataPower

Para poder configurar el Monitoring Agent for DataPower, debe completar algunas tareas de configuración en los dispositivos.

Consejo: Para obtener información sobre los dispositivos DataPower soportados, consulte la pestaña de requisitos previos en Informes de compatibilidad de productos de software.

Puede supervisar dispositivos DataPower a tres niveles diferentes. Configure los tres niveles según sus necesidades en cada Dispositivo DataPower que desee supervisar para visualizar datos de Dispositivo DataPower en la Consola de Cloud APM.

1. Supervisión de recursos

   Para ver datos de supervisión, como por ejemplo la utilización de recursos, el rendimiento y las estadísticas de conexión, habilite la supervisión de recursos. Para obtener instrucciones, consulte "Supervisión de recursos" en la página 241.

2. Rastreo de transacciones de middleware

   Para ver datos de supervisión de transacciones, como por ejemplo información detallada de transacción, volumen y dependencias, habilite el rastreo de transacciones de middleware. Si desea más instrucciones, consulte "Rastreo de transacciones de middleware" en la página 242.

3. Rastreo de transacciones a nivel de instancia del Dispositivo DataPower

   Para visualizar datos de supervisión para las transacciones en topologías de instancia, configure el rastreo de transacciones a nivel de instancia del Dispositivo DataPower. Si desea más instrucciones, consulte "Rastreo de transacciones de nivel de instancia de Dispositivo DataPower" en la página 243.

Importante: Asegúrese de que el ID de usuario tiene los permisos adecuados para configurar el Dispositivo DataPower. Puede especificar `*/*/*?Access=r` en el **Perfil de acceso** para el ID de usuario utilizado para configura el Dispositivo DataPower. Después puede utilizar este ID para configurar el Dispositivo DataPower.

Exportación del certificado público
Si la interfaz de gestión XML del dispositivo DataPower tiene el Perfil proxy SSL habilitado, debe exportar el certificado público que utiliza la interfaz de gestión XML del dispositivo DataPower en el sistema que ejecuta el Agente de DataPower .

Procedimiento

1. Para descargar el certificado cifrado que utiliza la interfaz de gestión XML del dispositivo Dispositivo DataPower, por ejemplo, `pubcert:///mycert.pem`, pulse **Administración** > **Principal** > **Gestión de archivos** y guarde el certificado en la máquina que ejecuta el Agente de DataPower .
2. Cuando configura el Agente de DataPower , hay una opción para especificar el campo **Perfil de proxy SSL**. Especifique la vía de acceso absoluta del certificado público.

   Nota: Cuando se añaden más pasarelas de varios protocolos, debe repetir estos pasos.

Supervisión de recursos
El primer nivel de supervisión disponible para un Dispositivo DataPower es habilitar la supervisión de recursos, como gestión de SOAP, estadística y velocidades de transacción.

Las operaciones realizadas en la interfaz de usuario (IU) de DataPower Gateway de las tareas de configuración siguientes corresponde a DataPower Gateway Versión 7.5.1 y versiones anteriores. Si la versión de DataPower Gateway que utiliza es posterior a V 7.5.1, puede pulsar el signo de interrogación de la esquina superior derecha de la IU y elegir **WebGUI** para volver a la IU de la versión anterior. A continuación, siga las instrucciones para completar las tareas de configuración del dispositivo DataPower.

Habilitación de la gestión SOAP
Si desea que Agente de DataPower recopile datos de dispositivos DataPower, deberá configurar la interfaz de gestión XML y habilitar la gestión SOAP.

Procedimiento

Para habilitar SOAP:

1. Inicie una sesión en la WebGUI para el dispositivo DataPower que desea supervisar.
2. Pulse **Objetos** > **Gestión de dispositivos** > **Interfaz de gestión XML**.

   Nota: Asegúrese de que el estado de administración esté habilitado.
3. Para **Número de puerto**, especifique el número de puerto en el que el Agente de DataPower está a la escucha de los informes de notificación. El número de puerto es 5550 de forma predeterminada.
4. Para **Servicios habilitados**, asegúrese de que **Gestión SOAP** esté seleccionado.

Habilitación de estadísticas
Si desea que Agente de DataPower recopile datos de dispositivos DataPower, las estadísticas deben estar habilitadas.

Procedimiento

Para habilitar las estadísticas, siga estos pasos:

1. Inicie una sesión en la WebGUI para el dispositivo DataPower que desea supervisar.
2. Pulse **Administración** > **Dispositivo** > **Configuración de estadísticas**.
3. Habilite **Valores de estadísticas** y pulse **Aplicar**.

Habilitación de Tasa de transacciones
Si desea que Agente de DataPower recopile datos de dispositivos DataPower, la Tasa de transacciones debe estar habilitada.

Procedimiento

Para habilitar la Tasa de transacciones, siga estos pasos:

1. Inicie una sesión en la WebGUI para el dispositivo DataPower que desea supervisar.
2. Seleccione el dominio `predeterminado`.
3. Pulse **Estado** > **Conexión** > **Tasa de transacciones**.
4. Si se visualiza **Las estadísticas están inhabilitadas actualmente**, pulse **inhabilitado** y, en Valores de estadísticas, establezca el **Estado de administración** en **habilitado**.
5. Si tiene varios dominios, pulse **Mostrar todos los dominios** y repita los pasos 3-4 para habilitar la Tasa de transacciones para todos los dominios pertinentes.
6. Pulse **Aplicar**.

Rastreo de transacciones de middleware
El segundo nivel de supervisión disponible para un Dispositivo DataPower es mostrar el rastreo de transacciones de middleware en los espacios de trabajo.

Las operaciones realizadas en la interfaz de usuario (IU) de DataPower Gateway de las tareas de configuración siguientes corresponde a DataPower Gateway Versión 7.5.1 y versiones anteriores. Si la versión de DataPower Gateway que utiliza es posterior a V 7.5.1, puede pulsar el signo de interrogación de la esquina superior derecha de la IU y elegir **WebGUI** para volver a la IU de la versión anterior. A continuación, siga las instrucciones para completar las tareas de configuración del dispositivo DataPower.

Se da soporte al rastreo de transacciones de tráfico SOAP y de tráfico REST a través del dispositivo DataPower. El rastreo de transacciones DataPower da soporte a SOAP utilizando archivos `store:///soapreq.xsl`, `store:///soaprsp.xsl` y `store:///soaperror.xsl`. Estos archivos XSL instrumentan el Proxy de servicio web para añadir y e informar sobre `kd4:KD4SoapHeaderV2` en el sobre SOAP.

Además de los archivos SOAP`*.xsl`, el rastreo de transacciones DataPower también incluye `apm_req.xsl`, `apm_rsp.xsl` y `apm_error.xsl`, que soportan solicitudes HTTP entrantes que contienen una `cabecera ARM_CORRELATOR: HTTP`, o un sobre SOAP que contiene `ITCAMCorrelator` o `kd4:KD4SoapHeaderV2`. El Proxy de servicio web actualiza o establece la solicitud de salida para contener una `cabecera ARM_CORRELATOR: HTTP` y elimina los correlacionadores SOAP.

Nota: Si se añaden dispositivos DataPower a una aplicación empresarial y el dispositivo lleva tráfico para múltiples aplicaciones, después de habilitar el rastreo de transacciones, la topología de aplicación que se visualiza para esas aplicaciones empresariales incluye vías de acceso a nodos para todas las aplicaciones.

Configuración de Web Service Management
Siga estos pasos para cada Dispositivo DataPower para el que desea visualizar datos de seguimiento.

1. Inicie una sesión en la WebGUI para el dispositivo DataPower que desea supervisar.

2. Seleccione el dominio predeterminado.
3. Busque Interfaz de gestión XML. Establezca los valores siguientes y pulse **Aplicar**.
   - En la pestaña **Principal**, en la sección **Servicios habilitados**, habilite **Punto final de WS-Management**
4. Busque Agente de gestión de Web Services. Establezca los valores siguientes y pulse **Aplicar**.
   - Establezca el **Estado administrativo** en **habilitado**
   - Establezca la **Modalidad de captura** en **Ninguna**
   - Establezca la **Modalidad de almacenamiento intermedio (en desuso)** en **Descartar**
5. Configure el proxy de servicio web o la pasarela multiprotocolo tal como se describe en los temas siguientes.

Configuración del proxy de servicio web
Complete estos pasos para cada proxy de servicio web para el que desee visualizar datos de seguimiento.

Procedimiento

1. Seleccione el dominio del que forma parte el proxy de servicio web.
2. En la pestaña **Valores de Proxy**, establezca los valores siguientes y pulse **Aplicar**:
   - Establezca **Supervisar mediante el agente de gestión de Web Services** en **activado**
3. Para informar de errores SOAP, inhabilite el proceso de errores y habilite la creación de informes de error en Consola de Cloud APM: en la pestaña **Valores avanzados de proxy**, establezca **Procesar errores HTTP** en off, y pulse **Aplicar**.

Configuración de la pasarela multiprotocolo
Siga estos pasos para cada pasarela multiprotocolo para la que desea visualizar datos de rastreo de transacciones.

Procedimiento

1. Seleccione el dominio del que forma parte la pasarela multiprotocolo.
2. En la pestaña **Avanzado** de la pasarela multiprotocolo, establezca los valores siguientes y pulse **Aplicar**:
   - Establezca **Supervisar mediante el agente de gestión de Web Services** en **activado**
   - Si el servidor web utiliza redireccionamiento, establezca **Seguir redireccionamientos** en **desactivado**. A continuación, establezca **Regrabar URL de ubicación** en **activado**.
3. Si está supervisando una pasarela multiprotocolo con Tipo de respuesta o Tipo de solicitud de no XML, debe definir una política de pasarela multiprotocolo con reglas que cubran tanto la dirección Cliente Servidor como Servidor Cliente. Si una pasarela multiprotocolo no XML no tiene reglas en su política, el agente de gestión de Web Services o un analizador de depuración DataPower no capturan tráfico (si están habilitados).
4. Para propagar el código de respuesta HTTP desde el servidor de fondo e informar de errores de SOAP, en la pestaña **Configuración avanzada**, establezca **Procesar errores de fondo** en desactivado y pulse **Aplicar**.

Rastreo de transacciones de nivel de instancia de Dispositivo DataPower
El tercer nivel de supervisión disponible para un Dispositivo DataPower es mostrar sus datos en topologías de instancias.

Las operaciones realizadas en la interfaz de usuario (IU) de DataPower Gateway de las tareas de configuración siguientes corresponde a DataPower Gateway Versión 7.5.1 y versiones anteriores. Si la versión de DataPower Gateway que utiliza es posterior a V 7.5.1, puede pulsar el signo de interrogación de la esquina superior derecha de la IU y elegir **WebGUI** para volver a la IU de la versión anterior. A continuación, siga las instrucciones para completar las tareas de configuración del dispositivo DataPower.

Configuración de transformaciones
Complete estos pasos en cada Dispositivo DataPower que desee visualizar en topologías de instancias.

Acerca de esta tarea

Para IBM Performance Management V8.1.2 Fixpack 1, se da soporte al rastreo de transacciones de tráfico SOAP a través del dispositivo DataPower. El rastreo de transacciones DataPower da soporte a SOAP utilizando archivos `store:///soapreq.xsl`, `store:///soaprsp.xsl` y `store:///soaperror.xsl`. Estos archivos XSL instrumentan el Proxy de servicio web para añadir y e informar sobre `kd4:KD4SoapHeaderV2` en el sobre SOAP.

Para IBM Performance Management V8.1.3 y posterior, también se da soporte al rastreo de transacciones de tráfico REST a través del dispositivo DataPower. Además de los archivos `SOAP*.xsl`, el rastreo de transacciones DataPower también incluye `apm_req.xsl`, `apm_rsp.xsl` y `apm_error.xsl`, que soportan solicitudes HTTP entrantes que contienen una `cabecera ARM_CORRELATOR: HTTP`, o un sobre SOAP que contiene `ITCAMCorrelator` o `kd4:KD4SoapHeaderV2`. El Proxy de servicio web actualiza o establece la solicitud de salida para contener una `cabecera ARM_CORRELATOR: HTTP` y elimina los correlacionadores SOAP.

El Agente de DataPower admite el rastreo de transacciones para el tráfico SOAP a través del dispositivo DataPower, el tráfico REST a través del dispositivo DataPower y el tráfico entre DataPower y WebSphere MQ.

- Si desea habilitar el rastreo de transacciones para el tráfico SOAP y REST a través del dispositivo DataPower, aplique `apm_req.xsl`, `apm_rsp.xsl` y `apm_error.xsl`, que admite las solicitudes HTTP de entrada que contienen una `cabecera ARM_CORRELATOR: HTTP` o un sobre SOAP que contiene `ITCAMCorrelator` o `kd4:KD4SoapHeaderV2`. El Proxy de servicio web actualiza o establece la solicitud de salida para contener una `cabecera ARM_CORRELATOR: HTTP` y elimina los correlacionadores SOAP.
- Además del tráfico SOAP y REST a través del dispositivo DataPower, si desea habilitar el rastreo de transacciones entre DataPower y WebSphere MQ, aplique los archivos `apm_req_MQ.xsl`, `apm_rsp_MQ.xsl` y `apm_error_MQ.xsl`. El rastreo de transacciones para el tráfico SOAP y REST también se habilita automáticamente tras aplicar estos archivos.

Procedimiento

Para rastrear el tráfico REST y habilitar el rastreo de transacciones entre DataPower y WebSphere MQ, siga estos pasos:

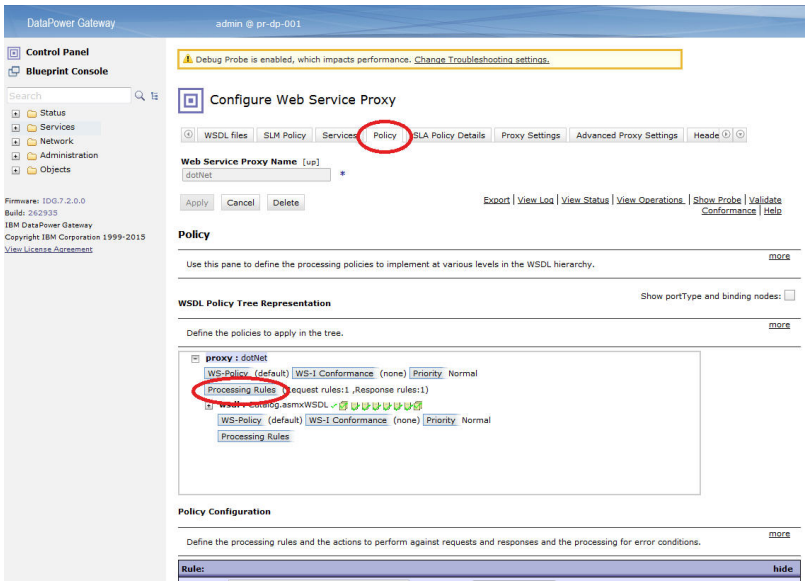
1. Descargue los archivos de la siguiente ubicación:
   - En sistemas Linux, `/opt/ibm/apm/agent/`*`lx8266`*`/bn/bin`
   - En sistemas AIX, `/opt/ibm/apm/agent/`*`aix536`*`/bn/bin`
2. Suba los archivos XSL a cada Dispositivo DataPower que desee supervisar como parte de la Pila de integración de IBM.
3. Configure el proxy de servicio web o la pasarela multiprotocolo tal como se describe en los temas siguientes.
4. Para cada dominio que desee supervisar, configúrelo con los pasos siguientes:
   a) Seleccione el Dominio de la lista desplegable en la cabecera de DataPower Gateway.
   b) En el navegador Panel de control, seleccione **Objetos** > **Gestión de dispositivos** > **Agente de gestión de Web Services**.
   c) Establezca la **Modalidad de almacenamiento intermedio (en desuso)** en `Descartar`.
   d) Pulse **Aplicar**.

Configuración del proxy de servicio web
Complete estos pasos en cada proxy de servicio web que desee visualizar en topologías de instancias.

Procedimiento

En la WebGUI, complete estos pasos para cada proxy de servicio web que desee supervisar:

1. En la página **Configurar proxy de servicio web**, seleccione el nombre del proxy de servicio web a configurar.
2. En la pestaña **Política**, expanda **proxy : *dominio*** y pulse **Reglas de proceso**.



3. En la sección **Configuración de política**, seleccione una regla `Cliente a servidor` existente, o pulse **Nueva regla** para crear una.

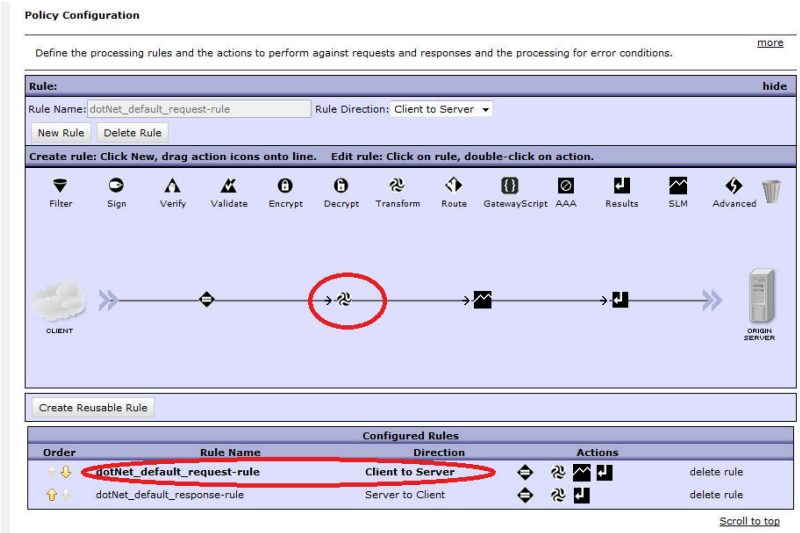
   a. Arrastre una transformación a la línea temporal.

   Nota:

   1) Si ya existe una regla `Cliente a servidor`, añádale el nodo de transformación.

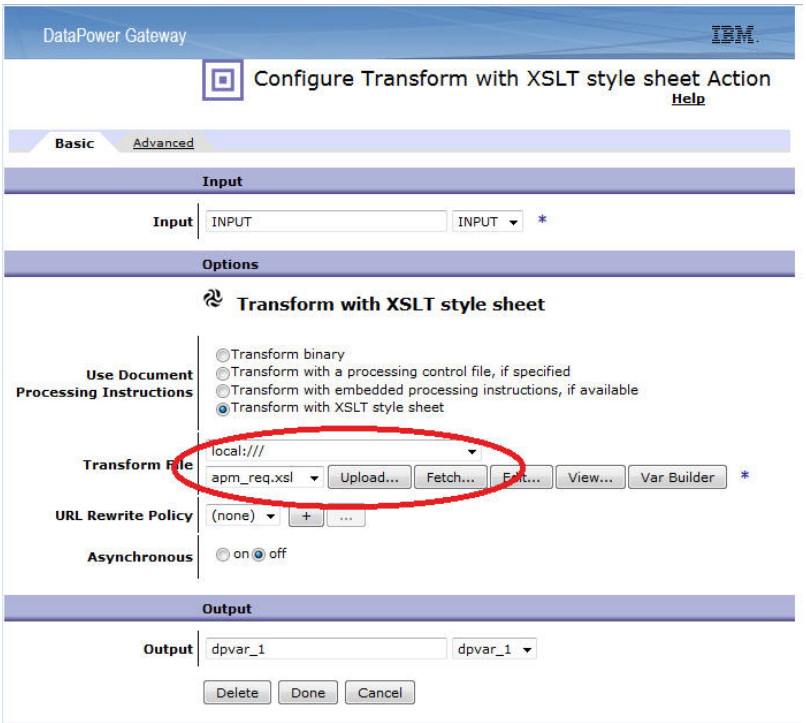
   2) Si la regla `Cliente a servidor` tiene un nodo de Autenticación, Autorización y Auditoría (AAA), asegúrese de que el nodo de transformación que incluye el archivos xslt del agente de DataPower preceda al nodo AAA.

   b. Efectúe una doble pulsación en la transformación para editarla.



   c. En la ventana **Configurar Acción de transformación con hoja de estilo XSLT**, al lado de Archivo de transformación, seleccione `apm_req.xsl` en el almacén de datos al que lo ha subido. Por ejemplo, `local:///`

   Si el archivo no existe, pulse **Subir** para obtenerlo de la ubicación de instalación.



Consejo: Además del tráfico de SOAP y REST a través del dispositivo DataPower, si desea configurar una regla de `Cliente a servidor` para supervisar el tráfico entre DataPower y WebSphere MQ, aplique el archivo `apm_req_MQ.xsl` en lugar del archivo `apm_req.xsl` en este paso.

d. Pulse **Realizado**.

4. De vuelta a la sección **Configuración de política**, repita el paso 3 para configurar una regla `Servidor a cliente` o pulse **Nueva regla** para crear una.

   a. Arrastre una transformación a la línea temporal.

   b. Efectúe una doble pulsación en la transformación para editarla.

   c. En la ventana **Configurar Acción de transformación con hoja de estilo XSLT**, al lado de Archivo de transformación, seleccione `apm_rsp.xsl` en el almacén de datos al que lo ha subido. Por ejemplo, `local:///`

   Si el archivo no existe, pulse **Subir** para obtenerlo de la ubicación de instalación.

   Consejo: Además del tráfico de SOAP y REST a través del dispositivo DataPower, si desea configurar una regla `Servidor a cliente` para supervisar el tráfico entre DataPower y WebSphere MQ, aplique el archivo `apm_rsp_MQ.xsl` en lugar del archivo `apm_rsp.xsl` en este paso.

   d. Pulse **Realizado**.

5. De vuelta a la sección **Configuración de política**, repita el paso 3 para configurar una regla `Error` o pulse **Nueva regla** para crear una.

   a. Arrastre una transformación a la línea temporal.

   b. Efectúe una doble pulsación en la regla de transformación para editarla.

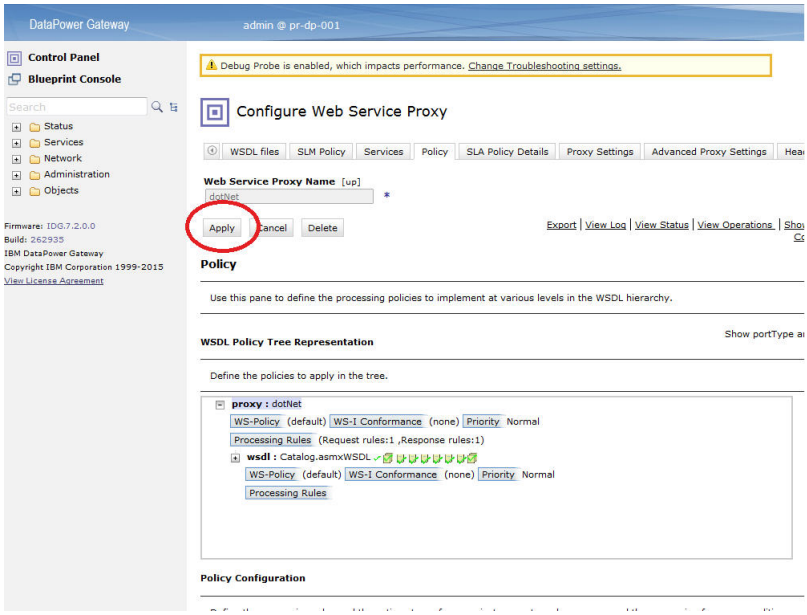
   c. En la ventana **Configurar Acción de transformación con hoja de estilo XSLT**, al lado de Archivo de transformación, seleccione `apm_error.xsl` en el almacén de datos al que lo ha subido. Por ejemplo, `local:///`

   Si el archivo no existe, pulse **Subir** para obtenerlo de la ubicación de instalación.

   Consejo: Además del tráfico SOAP y REST a través del dispositivo DataPower, si desea configurar una regla `error` para supervisar el tráfico entre DataPower y WebSphere MQ, aplique el archivo `apm_error_mq.xsl` en lugar del archivo `apm_error.xsl` en este paso.

d. Pulse **Realizado**.

6. De nuevo en la página **Configurar proxy de servicio web**, pulse **Aplicar**.



Configuración de la pasarela multiprotocolo

Complete estos pasos en cada pasarela multiprotocolo que desee visualizar en topologías de instancias.

Procedimiento

En la WebGUI, complete estos pasos para cada pasarela multiprotocolo que desee supervisar.

1. En la página **Configurar pasarela multiprotocolo**, pulse en el nombre de la pasarela multiprotocolo que desea configurar.
2. En la página **Política de pasarela multiprotocolo**, configure la política. Pulse **...**.
3. En la página **Configurar política de estilo de pasarela multiprotocolo**, seleccione una regla `Cliente a servidor` existente, o pulse **Nueva regla** para crear una.

   a. Arrastre una transformación a la línea temporal.

   Nota:

   1) Si ya existe una regla `Cliente a servidor`, añádale el nodo de transformación.
   2) Si la regla `Cliente a servidor` tiene un nodo de Autenticación, Autorización y Auditoría (AAA), asegúrese de que el nodo de transformación que incluye el archivos xslt del agente de DataPower preceda al nodo AAA.

   b. Efectúe una doble pulsación en la regla de transformación para editarla.

   c. En la ventana **Configurar Acción de transformación con hoja de estilo XSLT**, al lado de Archivo de transformación, seleccione `apm_req.xsl` en el almacén de datos al que lo ha subido. Por ejemplo, `local:///`

   Si el archivo no existe, pulse **Subir** para obtenerlo de la ubicación de instalación.

   Consejo: Además del tráfico de SOAP y REST a través del dispositivo DataPower, si desea configurar una regla de `Cliente a servidor` para supervisar el tráfico entre DataPower y WebSphere MQ, aplique el archivo `apm_req_MQ.xsl` en lugar del archivo `apm_req.xsl` en este paso.

   d. Pulse **Realizado**.

4. De nuevo en la página **Configurar política de estilo de pasarela multiprotocolo**, seleccione una regla `Servidor a cliente` existente, o pulse **Nueva regla** para crear una.

   a. Arrastre una transformación a la línea temporal.

b. Efectúe una doble pulsación en la regla de transformación para editarla.

c. En la ventana **Configurar Acción de transformación con hoja de estilo XSLT**, al lado de Archivo de transformación, seleccione `apm_rsp.xsl` en el almacén de datos al que lo ha subido. Por ejemplo, `local:///`

   Si el archivo no existe, pulse **Subir** para obtenerlo de la ubicación de instalación.

   Consejo: Además del tráfico de SOAP y REST a través del dispositivo DataPower, si desea configurar una regla `Servidor a cliente` para supervisar el tráfico entre DataPower y WebSphere MQ, aplique el archivo `apm_rsp_MQ.xsl` en lugar del archivo `apm_rsp.xsl` en este paso.

d. Pulse **Realizado**.

5. De nuevo en la página **Configurar política de estilo de pasarela multiprotocolo**, seleccione una regla `Error` existente, o pulse **Nueva regla** para crear una.

   a. Arrastre una transformación a la línea temporal.

   b. Efectúe una doble pulsación en la regla de transformación para editarla.

   c. En la ventana **Configurar Acción de transformación con hoja de estilo XSLT**, al lado de Archivo de transformación, seleccione `apm_error.xsl` en el almacén de datos al que lo ha subido. Por ejemplo, `local:///`

      Si el archivo no existe, pulse **Subir** para obtenerlo de la ubicación de instalación.

      Consejo: Además del tráfico SOAP y REST a través del dispositivo DataPower, si desea configurar una regla `error` para supervisar el tráfico entre DataPower y WebSphere MQ, aplique el archivo `apm_error_mq.xsl` en lugar del archivo `apm_error.xsl` en este paso.

   d. Pulse **Realizado**.

6. De nuevo en la página **Configurar política de estilo de pasarela multiprotocolo**, en la pestaña **Avanzados**, establezca **Supervisar mediante el agente de gestión de Web Services** en **activado** y pulse **Aplicar**.
7. Pulse **Aplicar**.

Qué hacer a continuación

En algunos casos, la adición de transformaciones para el rastreo de transacciones puede hacer que DataPower cambie el valor de las cabeceras HTTP Content-Type. Es posible que vea páginas web con imágenes que no se cargan, o archivos binarios representados como texto HTML indescifrable.

El comportamiento de DataPower cambia cuando se compara una regla sin transformaciones XSL con una regla con una o más transformaciones XSL. Si el servicio maneja mensajes MIME, MTOM, XOP u otros mensajes codificados, este comportamiento puede ser el deseado, de lo contrario, modifique la configuración de DataPower para evitar este comportamiento.

Para evitar que DataPower modifique la cabecera HTTP Content-Type, establezca la variable var://service/mpgw/proxy-content-type en cada regla afectada:

1. Arrastre un objeto avanzado a la regla.
2. Efectúe una doble pulsación en el objeto avanzado para editarlo.
3. Seleccione **Establecer variable** y pulse **Siguiente**.
4. Especifique el nombre de variable `service/mpgw/proxy-content-type` y el valor de variable 1 y pulse **Hecho**.
5. Aplique los cambios de configuración del servicio y la política.
6. Repita los pasos 1-5 para cada regla afectada.

Configuración del Agente de DataPower

Monitoring Agent for DataPower proporciona un punto central de supervisión para Dispositivos DataPower en su entorno de empresa. Puede identificar y recibir notificaciones sobre problemas

comunes con los dispositivos. El agente también proporciona información sobre rendimiento, recursos y carga de trabajo de los dispositivos.

Acerca de esta tarea

El agente DataPower es un agente de varias instancias; debe crear la primera instancia e iniciar el agente de forma manual. El Nombre de sistema gestionado incluye el nombre de instancia que especifique, por ejemplo, *nombre_instancia*:*nombre_host*:*pc*, donde *pc* es el código de producto de dos caracteres. El Nombre de sistema gestionado está limitado a 32 caracteres.

El nombre de instancia que especifique está limitado a 28 caracteres menos la longitud del nombre de host. Por ejemplo, si especifica `DataPower` como nombre de instancia, el nombre de sistema gestionado será `DataPower:nombrehost:BN`.

Importante: Si especifica un nombre de instancia largo, el Nombre de sistema gestionado queda truncado y el código de agente no se visualiza correctamente.

Nota: El XSLT del agente de DataPower no analiza los caracteres BLOB que se utilizan para aplicaciones de sistema principal.

Para cada Dispositivo DataPower de producción, configure una instancia. Si los dispositivos DataPower no son de producción o son pequeños, puede configurar una sola instancia de agente para supervisarlos todos. Varias instancias se pueden ejecutar en la misma máquina. Puede ejecutar el script de configuración para crear una instancia y cambiar los valores de configuración. Puede editar el archivo de respuestas silencioso de agente antes de ejecutar el script para saltarse las solicitudes y respuestas que en otro caso serían necesarias.

Procedimiento

- Para configurar el agente DataPower, complete uno de los procedimientos siguientes:
  - Linux AIX Para configurar el agente mediante respuestas a las solicitudes, siga estos pasos:
    1. Vaya al directorio *dir_instalación*`/bin`, donde *dir_instalación* es el directorio de instalación para el agente de DataPower.
    2. Ejecute el mandato `./datapower-agent.sh config` *nombre_instancia*.

       Seleccione un *nombre_instancia* que sea exclusivo en el servidor.
    3. Cuando se le solicite editar los valores del agente de DataPower, especifique 1 para continuar.
    4. Cuando se le solicite editar los **`Detalles del sistema gestionado`**, especifique una de las opciones siguientes:

       - `1=Añadir`
       - `2=Editar`
       - `3=Supr`
       - `4=Siguiente`
       - `5=Salir`

       Si es la primera vez que configura una instancia de agente de DataPower en el sistema, se visualizará el mensaje `No hay valores de 'DataPower Appliances' disponibles`. Especifique 1 para añadir un valor de DataPower Appliances. La opción predeterminada es `5=Salir`.
    5. Especifique las propiedades para el dispositivo DataPower:

       Nombre de sistema gestionado
       Para el **`Nombre de sistema gestionado`**, especifique el nombre del sistema gestionado del agente.

       Seleccione un **`Nombre de sistema gestionado`** que sea exclusivo en todas las instancias del agente y que se pueda utilizar para identificar fácilmente un dispositivo. El

nombre debe contener sólo caracteres alfanuméricos, por ejemplo, el nombre de host del Dispositivo DataPower.

Host de dispositivo
Para **Host de dispositivo**, indique la dirección IP del dispositivo DataPower supervisado. La dirección IP predeterminada es *9.123.109.139*.

Puerto de interfaz de gestión de XML
Para **Puerto de interfaz de gestión de XML**, especifique el número de puerto para la interfaz de gestión de XML. El número predeterminado es 5550.

ID de usuario
Para **ID de usuario**, escriba el ID de usuario para iniciar la sesión en el dispositivo DataPower supervisado. El valor predeterminado es admin.

Contraseña
Para **Contraseña**, especifique la contraseña para iniciar la sesión en el dispositivo DataPower supervisado y, a continuación, confirme la contraseña.

Perfil de proxy SSL
Para **Perfil de proxy SSL**, especifique la vía de acceso absoluta del certificado público para su perfil de proxy SSL, si la interfaz de gestión XML del dispositivo está configurada para utilizar el perfil. Por ejemplo,

```
la ubicación del archivo .pem exportado desde dispositivos datapower/mycert.pem
```

donde *la ubicación del archivo .pem exportado desde dispositivos datapower* es la vía de acceso absoluta del certificado público. Para exportar el certificado público, consulte Exportación del certificado público.

Opción de proxy SSL
Para **Opción de proxy SSL**, establezca Sí si la interfaz de gestión XML del dispositivo supervisado está configurada para utilizar un perfil de proxy SSL personalizado. De lo contrario, establézcalo en No.

6. Para supervisar varios dispositivos DataPower, repita los pasos "4" en la página 249 y "5" en la página 249 para configurar una instancia de agente para cada dispositivo DataPower. De lo contrario, especifique 5 y pulse **Intro** para completar la configuración.
7. Ejecute el mandato siguiente para iniciar el agente:

```
./datapower-agent.sh start nombre_instancia
```

- Configuración silenciosa

1. Para configurar el agente mediante la edición del archivo de respuestas silencioso y la ejecución del script sin interacción, siga estos pasos:
   - Linux AIX Abra *dir_instalación*/samples/datapower_silent_config.txt en un editor de texto.
   - Windows Abra *dir_instalación*\samples\datapower_silent_config.txt en un editor de texto.
2. Para configurar el agente DataPower para supervisar un dispositivo, especifique las propiedades siguientes:

Host de dispositivo
Especifique el nombre de host o la dirección IP del dispositivo. Por ejemplo, **SOAP_HOST.ManageSystemName=** *datapower01*.

Puerto de interfaz de gestión de XML
Entre el número de puerto de interfaz de gestión de XML. El valor predeterminado es 5550. Por ejemplo, **DP_PORT.ManageSystemName=** *5550*.

ID de usuario
Escriba el ID de usuario que se utiliza para conectarse al dispositivo. El valor predeterminado es admin. Por ejemplo, **DP_UID.ManageSystemName=** *admin*.

Contraseña
Escriba la contraseña del ID de usuario. Por ejemplo, **DP_PASSWORD.ManageSystemName=** *contraseña*.

Perfil de proxy SSL
Especifique la vía de acceso absoluta del certificado público para su perfil de proxy SSL, si la interfaz de gestión XML del dispositivo está configurada para utilizar el perfil. Por ejemplo,

```
la ubicación del archivo .pem exportado desde dispositivos datapower/mycert.pem
```

donde *la ubicación del archivo .pem exportado desde dispositivos datapower* es la vía de acceso absoluta del certificado público. Para exportar el certificado público, consulte Exportación del certificado público.

Opción de proxy SSL
Para **Opción de proxy SSL**, establezca Sí si la interfaz de gestión XML del dispositivo supervisado está configurada para utilizar un perfil de proxy SSL personalizado. De lo contrario, establézcalo en No. Por ejemplo, **DP_SSL_OPTION.ManageSystemName1=** Sí.

Importante: ManageSystemName es exclusivo. Debe sustituirlo por el nombre de su propio sistema en todas las entradas. Si desea supervisar varios dispositivos, copie y repita los pasos que se muestran para supervisar un dispositivo. Recuerde que debe establecer los correspondientes parámetros de ManageSystemName y DataPower Appliance.

3. Vaya al directorio de instalación del agente y ejecute el mandato siguiente para iniciar el agente:

```
./datapower-agent.sh start nombre_instancia
```

Qué hacer a continuación

- Para comprobar los nombres y valores de las instancias de agente configuradas, ejecute el mandato **./cinfo -s bn**.
- Puede verificar que los datos de Agente de DataPower se visualizan en la consola de Cloud APM. Si desea instrucciones sobre cómo iniciar la consola de Cloud APM, consulte la sección Inicio de la consola de Cloud APM. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte Gestión de aplicaciones.
- Para visualizar datos de rastreo de transacciones en la Consola de Cloud APM, configure el rastreo de transacciones para el Agente de DataPower . Para obtener instrucciones consulte Configuración del rastreo de transacciones para el agente DataPower.
- Para visualizar la supervisión en diferentes niveles, configure el Dispositivo DataPower en consecuencia. Para obtener instrucciones, consulte Supervisión de recursos, Rastreo de transacciones de middleware y Rastreo de transacciones a nivel de instancia de dispositivos DataPower.

Configuración del rastreo de transacciones para el Agente de DataPower
Para visualizar datos de rastreo de transacciones para los dispositivos DataPower en los paneles de instrumentos de middleware y topología, debe habilitar el rastreo de transacciones para el Agente de DataPower .

Antes de empezar

- Instale el Agente de DataPower y configúrelo para que se conecte al Dispositivo DataPower.
- Habilite la supervisión para SOAP o ARM en el Dispositivo DataPower.

Procedimiento

Para habilitar el rastreo de transacciones para el Agente de DataPower , siga estos pasos:

1. En la barra de navegación, pulse **Configuración del sistema** > **Configuración del agente**.
2. En la pestaña **DataPower**, seleccione las instancias de agente para las que desea habilitar el rastreo de transacciones.

3. Seleccione **Acciones** > **Establecer rastreo de transacciones** > **Habilitado** para habilitar el rastreo de transacciones. El estado del agente en la columna **Rastreo de transacciones** se actualizará a **Habilitado**.

Resultados
Ha habilitado el rastreo de transacciones para las instancias de agente seleccionadas.

Qué hacer a continuación
Para ver datos para un Dispositivo DataPower en los paneles de instrumentos de middleware y topología, ahora debe añadir los dispositivos que desea supervisar al Panel de instrumentos del rendimiento de aplicaciones. Para obtener más información sobre la adición de un Dispositivo DataPower en el Application Performance Dashboard, consulte "Adición de aplicaciones middleware al Application Performance Dashboard" en la página 102.

Nota: Si está utilizando Servicios de integración y desea supervisar los datos que se transmiten entre IBM Integration Bus y DataPower, se requiere configuración adicional para mostrar una topología precisa de transacciones agregadas. El Agente de IBM Integration Bus no puede incluir soporte de correlación para mensajes de SOAP sin un sobre SOAP. Los nodos `SOAPRequest`, `SOAPAsyncRequest` y `SOAPReply` pueden aceptar mensajes sin sobres SOAP como mensajes de entrada. Para estos nodos, no hay ninguna relación visualizada en la vista de topología desde la mediación a la mediación en sentido descendente o al servidor de aplicaciones. Para evitar este problema, inserte un nodo `SOAPEnvelope` inmediatamente antes de los nodos `SOAPRequest`, `SOAPAsyncRequest` o `SOAPReply` en el flujo de mensajes de IBM Integration Bus, y seleccione la opción **Crear nuevo sobre** para el nodo `SOAPEnvelope` para añadir un sobre SOAP para el mensaje SOAP.

Configuración de la supervisión de Db2

Monitoring Agent for Db2 supervisa la disponibilidad y el rendimiento del servidor de Db2. Puede supervisar varios servidores de Consola de Cloud APM; cada servidor está supervisado por una instancia de Agente de Db2. Agente de Db2 también da soporte a la supervisión remota.

Antes de empezar
Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Db2.

Acerca de esta tarea

Agente de Db2 es un agente de varias instancias. Primero debe crear la instancia y después iniciar manualmente el agente.

El nombre de sistema gestionado incluye el nombre de instancia de agente que especifique, por ejemplo *nombre_instancia*`:`*nombre_host*`:`*pc*.

Donde:

- *pc* es el código de producto de dos caracteres.
- *nombre_instancia* es el nombre de instancia de agente y debe ser el mismo nombre que el de la instancia de Db2 que se debe supervisar.

El nombre de sistema gestionado puede contener hasta 32 caracteres. El nombre de instancia de agente que especifique puede contener hasta 8 caracteres, excluida la longitud del nombre de host. Por ejemplo, si especifica `DB2inst1` como nombre de instancia de agente, el nombre de sistema gestionado será `DB2inst1:hostname:ud`.

Importante: Si especifica un nombre de instancia de agente largo, el nombre de sistema gestionado queda truncado y el código de agente no se visualiza correctamente.

Para evitar problemas de permisos al configurar el agente, asegúrese de utilizar el mismo ID de usuario root o no root que se utilizó para instalarlo. Si ha instalado el agente mediante un usuario seleccionado y

desea configurar el agente mediante un usuario distinto, consulte "Configuración de agentes como usuarios no root" en la página 191. Si ha instalado y configurado el agente mediante un usuario seleccionado y desea iniciar el agente mediante un usuario distinto, consulte "Inicio de agentes mediante un usuario no root" en la página 1047.

Ejecute el script de configuración para crear una instancia y cambiar los valores de configuración.Puede editar el archivo de respuestas silencioso de Db2 antes de ejecutar el script de configuración para ignorar las solicitudes y las respuestas que en otro caso serían necesarias.

Tras configurar el Agente de Db2, asegúrese de iniciar el agente con un ID de usuario que tenga la autoridad SYSADM de Db2 para la instancia supervisada. El agente requiere la autoridad SYSADM para activar todos los conmutadores de supervisor y recopilar los datos de supervisión. Por tanto, un usuario con la autoridad SYSADM debe iniciar el agente. Utilice el usuario propietario de la instancia, que tiene la autoridad SYSADM, para iniciar el agente.

Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Procedimiento

Para configurar el agente con los valores predeterminados, realice los pasos siguientes:

1. Ejecute el mandato siguiente, donde *nombre_instancia* es el nombre que desea proporcionar a la instancia:

   ```
   dir_instalación/bin/db2-agent.sh
   config nombre_instancia
    dir_instalación/samples/db2_silent_config.txt
   ```

   El nombre de instancia de agente *nombre_instancia* es siempre el mismo nombre que el de la instancia de Db2 que se está supervisando. Para obtener más detalles sobre las instancias de agente existentes, consulte "Página Configuración de agente" en la página 189.
2. Ejecute el mandato siguiente para iniciar el Agente de Db2:

   ```
   dir_instalación/bin/db2-agent.sh start nombre_instancia
   ```

Qué hacer a continuación

- Otorgue privilegios al usuario de Db2 para ver los datos de algunos atributos de Db2. Para obtener información sobre cómo otorgar estos privilegios, consulte "Cómo otorgar privilegios para visualizar métricas de Db2" en la página 258.
- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del agente en sistemas Windows

Puede utilizar la ventana de IBM Cloud Application Performance Management para configurar el agente en sistemas Windows.

Antes de empezar

Antes de empezar a configurar el Agente de Db2 para la supervisión local y remota, asegúrese de que se haya llevado a cabo la tarea siguiente para la supervisión remota.

- Configure el entorno de cliente/servidor para la supervisión remota, consulte "Requisitos previos para la supervisión remota" en la página 262.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. En la ventana IBM Cloud Application Performance Management, pulse el botón derecho del ratón en **Monitoring Agent for DB2** y luego pulse **Configurar agente**.
3. En el campo **Especificar un nombre de instancia exclusivo**, escriba el nombre de la instancia del agente y pulse **Aceptar**.

   Importante: Para la supervisión local, el nombre de la instancia de agente debe coincidir con el nombre de la instancia de Db2 que se está supervisando.

   Para la supervisión remota, el nombre de la instancia de agente debe ser el nombre de nodo de catálogo exclusivo.
4. En la ventana **Monitoring Agent for DB2**, complete estos pasos:
   a) En **Nombre de usuario**, escriba el nombre de usuario de la instancia de Db2.

      Para Db2 local, escriba el nombre del propietario de la instancia de Db2.

      Para Db2 remoto, escriba el nombre del propietario de la instancia de Db2 real de la máquina remota de Db2.

      Importante: Este parámetro es obligatorio para la supervisión de la instancia remota de Db2.

   b) En **Contraseña**, escriba la contraseña de la instancia de Db2.

      Para Db2 local, escriba la contraseña del propietario de la instancia local de Db2.

      Para Db2 remoto, escriba la contraseña del propietario de la instancia de Db2 real de la máquina remota de Db2.

      Importante: Este parámetro es obligatorio para la supervisión de la instancia remota de Db2.

   c) En el campo **Archivo de definición de SQL personalizado de DB2**, especifique el nombre completo de vía de acceso del archivo de definición SQL. Si el archivo de definición de SQL está en el directorio predeterminado, deje este campo en blanco. De lo contrario, especifique el nombre completo de vía de acceso del archivo. El nombre de archivo predeterminado con la vía de acceso es el siguiente:

      Linux AIX `CANDLEHOME/config/kudcussql.properties`

      Windows `CANDLEHOME\TMAITM6_x64\kudcussql.properties`

   d) En el campo **Vía de acceso de archivo de registro db2diag**, especifique la vía de acceso del directorio del archivo de registro db2diag. Si el archivo de registro db2diag se encuentra en el directorio predeterminado, deje este campo en blanco. De lo contrario, especifique la vía de acceso del directorio. La vía de acceso del directorio predeterminado es la siguiente:

      Linux AIX `/home/`*`DB2owner_home_dir`*`/sqllib/db2dump`

      Windows `C:\ProgramData\IBM\DB2\DB2COPY\`*`DB2INSTANCENAME`*

      Nota: Este parámetro no se aplica a la supervisión remota.

   e) En el campo **Filtro MSGID en expresión regular**, especifique *MSGID* para filtrar el registro de diagnóstico. El MSGID es una combinación del tipo, número y nivel de gravedad del mensaje. Utilice una expresión regular para filtrar el registro en función del tipo de mensaje, el número de mensaje o el nivel de gravedad, por ejemplo, `ADM1\d*1E|ADM222\d2W`.

   f) En la lista **Habilitar la supervisión para particiones en hosts remotos**, seleccione `Sí` para especificar que el Agente de Db2 puede supervisar particiones en hosts remotos.

   g) En la lista **Habilitar supervisión de todas las bases de datos**, seleccione `Sí` para especificar que el Agente de Db2 puede supervisar todas las bases de datos.

   h) Pulse **Aceptar**.

      La instancia de agente se visualiza en la ventana IBM Cloud Application Performance Management.

5. Ejecute los pasos siguientes para configurar la supervisión remota.
   a) Abra *dir_instalación*\TMAITM6_x64\KUDENV_<nombre_instancia>.
   b) Defina *KUD_DB2_CLIENT_INST* en el nombre de la instancia de cliente de Db2 bajo el que se ha catalogado la instancia remota del servidor de Db2.
6. Pulse el botón derecho del ratón en la instancia de **Monitoring Agent for DB2** y pulse **Iniciar**.

Qué hacer a continuación

- Otorgue privilegios al usuario de Db2 para ver los datos de algunos atributos de Agente de Db2. Para obtener información sobre cómo otorgar estos privilegios, consulte "Cómo otorgar privilegios para visualizar métricas de Db2" en la página 258.
- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del agente en sistemas Linux o UNIX

Ejecute el script de configuración para configurar el agente en sistemas Linux.

Antes de empezar

Antes de empezar a configurar el Agente de Db2 para la supervisión local y remota, asegúrese de que se haya llevado a cabo la tarea siguiente para la supervisión remota.

- Configure el entorno de cliente/servidor para la supervisión remota, consulte "Requisitos previos para la supervisión remota" en la página 262.

Procedimiento

1. Ejecute el mandato *dir_instalación*/bin/db2-agent.sh config *nombre_instancia*

   Donde *nombre_instancia* es el nombre que desea dar a la instancia:

   Importante: Para la supervisión local, el nombre de la instancia de agente debe coincidir con el nombre de la instancia de Db2 que se está supervisando.

   Para la supervisión remota, el nodo catalogado local de la instancia de servidor de Db2 remota que se debe supervisar.
2. Cuando se le solicite que proporcione un valor para los parámetros siguientes, presione la tecla Intro para aceptar el valor predeterminado o especifique un valor y luego presione la tecla Intro:
   - Nombre de usuario
   - Contraseña
   - Vía de acceso de SQL de DB2
   - Vía de acceso de Diaglog
   - Filtro de ID de mensaje de Diaglog
   - Supervisar particiones remotas
   - Supervisar todas las bases de datos
3. Ejecute el mandato siguiente para iniciar el agente:

   Para la supervisión local, ejecute *dir_instalación*/bin/db2-agent.sh start *nombre_instancia* a través del usuario propietario de la instancia de Db2.

   Para la supervisión remota, ejecute *dir_instalación*/bin/db2-agent.sh start *nombre_nodo* con el propietario de la instancia de la instancia de cliente de Db2 en la que se cataloga la instancia de servidor de Db2.

Qué hacer a continuación

- Otorgue privilegios al usuario de Db2 para ver los datos de algunos atributos del Agente de Db2. Para obtener información sobre cómo otorgar estos privilegios, consulte "Cómo otorgar privilegios para visualizar métricas de Db2" en la página 258.
- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del agente mediante el archivo de respuestas silencioso

Utilice el archivo de respuestas silencioso para configurar el agente sin responder a las solicitudes cuando ejecuta el script de configuración. Puede utilizar el archivo de respuestas silencioso para configurar el agente en sistemas Windows y Linux.

Antes de empezar

Antes de empezar a configurar el Agente de Db2 para la supervisión local y remota, asegúrese de que se haya llevado a cabo la tarea siguiente para la supervisión remota.

- Configure el entorno de cliente/servidor para la supervisión remota, consulte "Requisitos previos para la supervisión remota" en la página 262.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración. Puede editar los valores de estos parámetros en el archivo de respuestas y ejecutar el script de configuración para crear una instancia de agente y actualizar los valores de configuración.

Procedimiento

1. En un editor de texto, abra el archivo `db2_silent_config.txt` que está disponible en la siguiente vía de acceso:

   Linux AIX *dir_instalación*`/samples/db2_silent_config.txt`

   Windows *dir_instalación*`\tmaitm6_x64\samples\db2_silent_config.txt`
2. En el archivo de respuestas, especifique un valor para los parámetros siguientes:
   - En **Nombre de usuario**, escriba el nombre de usuario de la instancia de Db2.

     Para Db2 local, escriba el nombre del propietario de la instancia de Db2.

     Para Db2 remoto, escriba el nombre del propietario de la instancia de Db2 real de la máquina remota de Db2.

     Importante: Este parámetro es obligatorio para la supervisión de la instancia remota de Db2.
   - En **Contraseña**, escriba la contraseña de la instancia de Db2.

     Para Db2 local, escriba la contraseña del propietario de la instancia local de Db2.

     Para Db2 remoto, escriba la contraseña del propietario de la instancia de Db2 real de la máquina remota de Db2.

     Importante: Este parámetro es obligatorio para la supervisión de la instancia remota de Db2.
   - Para el parámetro **Vía de acceso de SQL de DB2**, deje este campo en blanco si el archivo de definición de SQL está disponible en el directorio predeterminado. De lo contrario, entre la vía de acceso del directorio correcta. El archivo de definición de SQL está disponible en la vía de acceso predeterminada siguiente:

     Linux AIX `CANDLEHOME/config/kudcussql.properties` Por ejemplo, **KUD_DB2_SQL_PATH=** `/opt/ibm/apm/agent/config/kudcussql.properties`

Windows CANDLEHOME\TMAITM6_x64\kudcussql.properties Por ejemplo, **KUD_DB2_SQL_PATH=** C:\IBM\ITM\TMAITM6_x64\kudcussql.properties

- Para el parámetro **vía de acceso al diálogo**, deje este campo en blanco si el archivo de registro db2diag está disponible en el directorio predeterminado. De lo contrario, entre la vía de acceso del directorio correcta. El archivo de registro está disponible en la vía de acceso predeterminada siguiente:

  Linux AIX /home/Dir_inicio_propietarioDB2/sqllib/db2dump
  Por ejemplo, **KUD_DIAGLOG_PATH=** /home/db2inst1/sqllib/db2dump.
  Windows Windows Install_Driver:\ProgramData\IBM\DB2\DB2COPY \DB2INSTANCENAME
  Por ejemplo, **KUD_DIAGLOG_PATH=** C:\ProgramData\IBM\DB2\DB2COPY1\DB2

  Nota: Este parámetro no se aplica a la supervisión remota.

- Para el parámetro **filtro de ID de mensaje de dialogo**, especifique *MSGID* para filtrar el registro de diagnóstico. El MSGID es una combinación del tipo, número y nivel de gravedad del mensaje. También puede utilizar una expresión regular, por ejemplo, **KUD_DIAGLOG_MSGID_FILTER=** ADM1\d*1E|ADM222\d2W.
- Para el parámetro **supervisar particiones remotas**, indique Yes para especificar que Agente de Db2 supervisará las particiones en los host remotos. Por ejemplo, **KUD_MONITOR_REMOTE_PARTITIONS=** *Yes*.
- Para el parámetro **supervisar todas las bases de datos**, indique Yes para especificar que desea que Agente de Db2 supervise todas las bases de datos. Por ejemplo, **KUD_MONITOR_ALL_DATABASES=** *Yes*.

3. Guarde y cierre el archivo db2_silent_config.txt y ejecute el mandato siguiente.

   Linux AIX *dir_instalación*/bin/db2-agent.sh config *nombre_instancia* *dir_instalación*/samples/
   db2_silent_config.txt
   Windows *dir_instalación*\bin\db2-agent.bat config*nombre_instancia* \tmaitm6_x64\samples\db2_silent_config.txt

   <nombre_instancia> es

   - Para la supervisión del servidor de Db2 local: el nombre de instancia del servidor de Db2 que desea supervisar.
   - Para la supervisión del servidor de Db2 remota: el nombre de nodo de catálogo de la instancia del servidor de Db2 remoto.

   Importante: Asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

4. Para Windows, abra el archivo CANDLEHOME\TMAITM6_x64\KUDENV_<nombre_instancia>. Y edite la línea, KUD_DB2_CLIENT_INST como KUD_DB2_CLIENT_INST=<nombre de instancia del cliente bajo el que se ha catalogado la instancia del servidor Db2 remoto>
5. Ejecute el mandato siguiente para iniciar el agente:

   Linux AIX *dir_instalación*/bin/db2-agent.sh start *nombre_instancia*
   Windows *dir_instalación*\bin\db2-agent.bat start nombre_instancia

   Recuerde: Mientras se supervisa la instancia del servidor de Db2 remoto desde UNIX o Linux, el mandato se debe ejecutar con el propietario de la instancia de cliente bajo el que se cataloga la instancia de servidor remoto.

Qué hacer a continuación

- Otorgue privilegios al usuario de Db2 para ver los datos de algunos atributos de Agente de Db2. Para obtener información sobre cómo otorgar estos privilegios, consulte "Cómo otorgar privilegios para visualizar métricas de Db2" en la página 258.
- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Cómo otorgar privilegios para visualizar métricas de Db2

Para supervisar los recursos de Db2, un usuario de Db2 debe tener autoridad SYSADM, SYSCTRL, SYSMAINT y SYSMON de Db2 sobre la instancia supervisada a fin de ver los datos de algunos atributos del Agente de Db2.

Acerca de esta tarea

Para ver los datos de supervisión que el agente recopila para todos los atributos en el panel de instrumentos, el usuario de Db2 debe tener privilegios específicos. Para asignar estos privilegios al usuario de Db2, ejecute el archivo de script que se encuentra en la ubicación siguiente:

Linux AIX *dir_instalación*/config/KudGrantUserPermissions.sh

Windows *dir_instalación*\TMAITM6_x64\KudGrantUserPermissions.bat

Un usuario de Db2 con la autoridad SYSADM puede ejecutar el script para otorgar privilegios a sí mismo o a cualquier otro usuario de Db2. Para una instancia de Db2, utilice el propietario de la instancia, que ya tiene autoridad SYSADM, para ejecutar el script con el fin de otorgar otros permisos a sí mismo o para otorgar todos los permisos a cualquier otro usuario de Db2.

Procedimiento

1. Para la supervisión local, consulte los pasos siguientes.
   a) En el sistema donde se ha instalado el Agente de Db2, abra la interfaz de línea de mandatos de Db2.
   b) Ejecute el mandato siguiente donde *nombre_instancia* es el nombre de la instancia de Db2 y *nombre_usuario* es el nombre del usuario de Db2:

      Linux AIX *dir_instalación*/config/KudGrantUserPermissions.sh *nombre_instancia nombre_usuario*

      Windows *dir_instalación*\TMAITM6_x64\KudGrantUserPermissions.bat *nombre_instancia nombre_usuario*

      Nota: Para sistemas Windows, *nombre_usuario* es opcional en el mandato. Si no se especifica un nombre de usuario en el mandato, los privilegios se asignan al usuario predeterminado (system).
2. Para la supervisión remota, consulte los pasos siguientes.
   a) Copie KudGrantUserPermissions.sh para Unix o Linux y KudGrantUserPermissions.bat para Windows desde *dir_instalación*/TMAITM6_x64/ en la estación de trabajo del agente en la máquina del servidor de Db2.
   b) Ejecute el mandato siguiente desde el usuario propietario de la instancia de Db2 cuyo *nombre_instancia* es el nombre de la instancia de Db2 y cuyo *nombre_usuario* es el nombre del usuario de Db2:

      Linux AIX ./KudGrantUserPermissions.sh *nombre_instancia nombre_usuario*

      Windows KudGrantUserPermissions.bat *nombre_instancia nombre_usuario*

      Recuerde: Para llevar a cabo una supervisión remota de Db2 en Windows, el *nombre_usuario* debe ser el nombre de usuario que se ha proporcionado durante la configuración del Agente de Db2 en la estación de trabajo de cliente.

Configuración de las variables del entorno local

Puede configurar variables de entorno local para cambiar el comportamiento del Agente de Db2.

Procedimiento

1. En sistemas Windows, pulse **Inicio**> **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, en el menú **Acciones**, pulse **Avanzada > Editar archivo ENV**.
3. En sistemas Linux o AIX, vaya a la línea de mandatos y edite el archivo ud.environment del directorio dir_instalación/config. Donde dir_instalación es el directorio de instalación del agente.

   Nota: El archivo ud.environment es un archivo oculto.
4. En el archivo de variables de entorno, especifique los valores de las variables de entorno.

   Para obtener información sobre las variables de entorno que puede configurar, consulte "Variables de entorno local" en la página 259.

Variables de entorno local

Puede cambiar el comportamiento del Agente de Db2 configurando las variables de entorno local.

Variables para definir el método de recopilación de datos para el conjunto de datos de espacio de tabla

Para establecer el método para la recopilación de datos del conjunto de datos de espacio de tabla, utilice las siguientes variables de entorno:

- **KUD_T1_BY_SQL**: utilice esta variable para establecer el método de recopilación de datos para el conjunto de datos de espacio de tabla utilizando consultas SQL. Para habilitar la recopilación de datos mediante consultas SQL, establezca el valor de esta variable en Y. Para recopilar datos para el conjunto de datos de espacio de tabla utilizando el método de instantánea, establezca el valor de esta variable en N. El valor predeterminado de esta variable es N.

  Importante: para recopilar datos utilizando consultas SQL, la versión de Db2 debe ser 9.7 o posterior. Además, el usuario que inicia el Agente de Db2 debe tener la autoridad SYSADM para todas las bases de datos.
- **KUD_T1_DISABLE**: utilice esta variable para inhabilitar la recopilación de datos para el conjunto de datos de espacio de tabla. Para habilitar la recopilación de datos para el conjunto de datos de espacio de tabla, establezca el valor de esta variable en N. Para inhabilitar la recopilación de datos para el conjunto de datos de espacio de tabla, establezca el valor de esta variable en Y. El valor predeterminado de esta variable es N.

Variable para excluir los nodos del recurso de almacenamiento en memoria caché (CF) de la recopilación de datos

Para excluir los nodos del recurso de almacenamiento en memoria caché (CF) del algoritmo de recopilación de datos en el entorno de pureScale, utilice la variable **DB2_CF_PARTITION_NUMS**. En el archivo de entorno del agente, establezca la variable **DB2_CF_PARTITION_NUMS** como DB2_CF_PARTITION_NUMS=<número de nodo de CF>. Por ejemplo, DB2_CF_PARTITION_NUMS=1. Para más de un nodo de CF, establezca el valor de variable **DB2_CF_PARTITION_NUMS** como una lista que utiliza cualquier símbolo especial de # . : , ; | @ como delimitador. Por ejemplo, DB2_CF_PARTITION_NUMS=12,13,23,34. No hay ningún valor predeterminado para esta variable.

Variable para limitar la recopilación de datos para el conjunto de datos Tabla de Db2

Para establecer el número máximo de filas que debe devolver Agente de Db2, al recopilar datos para el conjunto de datos Tabla de Db2, utilice la variable de entorno **KUD_TABLE_NUMBER**. El valor predeterminado es 10000.

Variable para establecer el intervalo de recarga del archivo de propiedades de SQL personalizado

Para establecer el intervalo de tiempo de recarga (en segundos) para el archivo de propiedades SQL personalizado, utilice la variable **KUD_CUS_SQL_INTERVAL**. El valor predeterminado es 20 segundos.

Variable para limitar las filas en la recopilación de datos para el conjunto de datos Suceso de agente

Para establecer el número de filas para la recopilación de datos del conjunto de datos Suceso de agente, utilice la variable **KUD_AGENT_EVENT_CACHE**. El conjunto de datos Suceso de agente proporciona información detallada sobre los sucesos predefinidos y desencadenados y determina los problemas de estado de la base de datos supervisada. El valor predeterminado es 50.

Variable para limitar las filas en la recopilación de datos para el conjunto de datos Registro de anotaciones de Db2

Para establecer el número de filas para la recopilación de datos del conjunto de datos Registros de anotaciones de the Db2, utilice la variable **KUD_DBHISTORY_MAXROW**. El conjunto de datos Registro de anotaciones de Db2 proporciona información histórica sobre el registro de archivado de Db2. El valor predeterminado es 500.

Variables para definir la recopilación de datos para el conjunto de datos Registro de diagnóstico de Db2

Para establecer el método para la recopilación de datos del conjunto de datos Registro de diagnóstico de Db2, utilice las siguientes variables de entorno:

- **KUD_DIAGLOG_BY_TABLE**: Utilice esta variable para establecer el método de recopilación de datos para el conjunto de datos Registro de diagnóstico de Db2. Si el valor de esta variable se establece en Y, los datos del conjunto de datos Registro de diagnóstico de Db2 se recopilarán utilizando consultas SQL. Si el valor de esta variable está establecido en N, los datos del conjunto de datos Registro de diagnóstico de Db2 se recopilarán analizando db2diag.log. El valor predeterminado de esta variable es Y.

  Importante: para recopilar datos utilizando consultas SQL, la versión de Db2 debe ser 10 o posterior.
- **KUD_DIAGLOG_TAILCOUNT**: utilice esta variable para definir el número de líneas del archivo db2diag.log que el Agente de Db2 analiza para recopilar datos para el conjunto de datos Registro de diagnóstico de DB2. Esta variable limita el Agente de Db2 a procesar el archivo de registro de Agente de Db2 de modo que sólo se supervisen los mensajes y los sucesos más recientes. El valor predeterminado de esta variable es 1000.
- **KUD_DIAGLOG_CACHE**: Utilice esta variable para limitar el número de registros de anotaciones que se muestran en el panel de instrumentos para el conjunto de datos Registro de diagnóstico de Db2. El valor predeterminado de esta variable es 20.
- **KUD_DIAGLOG_INTERVAL**: Utilice esta variable para definir el intervalo de tiempo de recarga (en segundos) del archivo db2diag.log para la recopilación de datos para el conjunto de datos Registro de diagnóstico de Db2. El valor predeterminado de esta variable es 30 segundos.
- **KUD_DISABLE_DIAGLOG**: Utilice esta variable para inhabilitar la recopilación de datos para el conjunto de datos Registro de diagnóstico de Db2. Para habilitar la recopilación de datos para el conjunto de datos Registro de diagnóstico de Db2, establezca el valor de esta variable en N. Para inhabilitar la recopilación de datos para el conjunto de datos Registro de diagnóstico de Db2, establezca el valor de esta variable en Y. El valor predeterminado de esta variable es N.

Variable para establecer el intervalo de tiempo de espera de consulta

Si una consulta SQL tarda mucho tiempo en completarse, afecta al rendimiento del Agente de Db2. Para establecer el intervalo de tiempo de espera de consulta para el Agente de Db2, utilice la variable **KUD_QUERY_TIMEOUT**. Utilice esta variable para definir la cantidad máxima de tiempo (en segundos) que el Agente de Db2 espera para recibir una respuesta a una consulta que se ha enviado al servidor de Db2. El valor de esta variable debe ser inferior a 300 segundos. El valor predeterminado de esta variable es 45 segundos.

Variable para definir la recopilación de datos para el conjunto DB2 Database01 (Reemplazado)

El agente no debe desencadenar consultas ASN para recopilar datos para el conjunto de datos DB2 Database01 (Reemplazado) cuando no existen esquemas ASN. Para habilitar la ejecución de las consultas ASN, utilice la variable **KUD_REPLICATION_ON**. Si el valor de esta variable se establece en Y, el Agente de Db2 ejecuta consultas ASN incluso cuando los esquemas ASN no están presentes. Si el valor de esta variable se establece en N, el Agente de Db2 no ejecuta las consultas ASN. El valor predeterminado de esta variable es Y.

Variable para configurar los conmutadores de supervisor al recopilar datos mediante el método de instantánea

Si desea recopilar los datos de supervisión del Agente de Db2 utilizando el método de instantánea, habilite el conmutador del supervisor de Db2 para el conjunto de datos. Para habilitar el conmutador del supervisor de Db2, utilice la variable **KUD_MON_SWITCH_OVERRIDE**. La lista de conmutadores del supervisor de Db2 es la siguiente:

LOCK
Información de bloqueo

SORT
Información sobre la clasificación

STATEMENT
Información de sentencias SQL

TABLE
Información de actividad de tabla

TIMESTAMP
Recopilar información de indicación de fecha y hora

UOW
Información de unidad de trabajo

Si el valor de esta variable se establece en Y, el Agente de Db2 conserva el valor de configuración de los conmutadores de supervisor de Db2. Si el valor de esta variable se establece en N, el Agente de Db2 habilita todos los conmutadores de supervisor para recopilar datos. El valor predeterminado de esta variable es N.

Variable para rastrear los datos del almacenamiento intermedio de instantánea de Db2 de un conjunto de datos

Para ver los datos que se recopilan para un conjunto de datos utilizando el método de instantánea, utilice la variable **KUD_SNAPSHOT_DUMPOUT**. Si el valor de esta variable se establece en Y, el Agente de Db2 vuelca los datos de almacenamiento intermedio de instantánea para grupos de atributos del archivo de registro del agente. Si el valor de esta variable se establece en N, el Agente de Db2 no vuelca los datos de almacenamiento intermedio de instantánea del archivo de registro del agente. El valor predeterminado de esta variable es N.

Variable para rastrear el Agente de Db2 utilizando los datos del almacenamiento intermedio de instantánea de un conjunto de datos

Para rastrear el Agente de Db2 utilizando los datos del almacenamiento intermedio de instantánea que se recopilan para un conjunto de datos, utilice la variable **KUD_SNAPSHOT_READIN**. Para habilitar el rastreo del Agente de Db2, establezca el valor de esta variable en Y. Para inhabilitar el rastreo del Agente de Db2, establezca el valor de esta variable en N.

Variable para definir el método de recopilación de datos para el conjunto de datos Conflicto de bloqueo.

Para establecer el método de recopilación de datos para el conjunto de datos Conflicto de bloqueo, utilice la variable **KUD_LOCKCONFLICT_BY_SQL**. Para recopilar datos para el conjunto de datos Conflicto de bloqueo mediante consultas SQL, establezca el valor de esta variable en Y. Para recopilar datos para el

conjunto de datos Conflicto de bloqueo mediante el método de instantánea, establezca el valor de esta variable en N. El valor predeterminado de esta variable es Y.

Importante: para recopilar datos utilizando consultas SQL, la versión de Db2 debe ser 9.7 FP1 o posterior. Además, el usuario que inicia el Agente de Db2 debe tener la autoridad SYSADM para todas las bases de datos.

Variable para supervisar servidor de Db2 remoto en Windows

KUD_DB2_CLIENT_INST: establezca esta variable en el nombre de instancia de cliente de Db2 bajo el que se cataloga la instancia de servidor de Db2 remota. Solo debe establecer esta variable si está utilizando la supervisión remota y el agente está en Windows.

Requisitos previos para la supervisión remota

Puede utilizar Monitoring Agent for Db2 para la supervisión remota. Consulte en el tema los requisitos previos de la supervisión remota de Db2.

Acerca de esta tarea

Para la supervisión remota de Db2, primero debe llevar a cabo la configuración del entorno básico cliente/servidor de Db2. Lleve a cabo esta configuración para Windows y UNIX o Linux.

Para realizar esta configuración, un usuario debe tener autoridad Db2 SYSADM o SYSCTRL.

Recuerde: Ejecute todos los pasos en la estación de trabajo de agente salvo el paso 2.

Procedimiento

1. En la estación de trabajo del Agente de Db2, instale el cliente de Db2. La versión de este cliente debe ser superior o igual a la de la versión de la instancia del servidor de Db2 que se debe supervisar.
2. Verifique que el protocolo de comunicación para la instancia de Db2 sea TCPIP.
   a) Para verificarlo, ejecute el mandato **db2set** en la `línea de mandatos` de Db2.
   b) Si no está establecido en TCPIP, ejecute **db2set DB2COMM=tcpip** en la `línea de mandatos` de Db2.

   Importante: Este paso se lleva a cabo en el lado del servidor.
3. Catalogue la instancia de servidor remoto en la estación de trabajo de agente de Db2 con el mandato siguiente.

   Importante: La instancia de servidor se debe catalogar bajo la instancia de cliente. Ejecute el mandato siguiente en la instancia de cliente.

   db2=>CATALOG TCPIP NODE<nombre_nodo> REMOTE <nombre_host/dirección_ip> SERVER <nombre_servicio/número_puerto>

   en Db2 donde

   a. *<nombre_nodo>* representa un apodo local de la instancia de Db2 en el componente de cliente.

      Nota: Para UNIX o Linux, *<nombre_nodo>* no debe ser el mismo que el de ningún cliente de Db2 ni de ningún nombre de instancia de servidor de Db2 que haya disponible en la misma estación de trabajo.

   b. <nombre_host/dirección_IP> representa el nombre o la dirección IP de la estación de trabajo del servidor de Db2.

   c. <nombre_servicio/número_puerto> en el que se ha configurado el TCIP de Db2.

   Para catalogar la instancia de servidor de Db2 que se está ejecutando en el número de puerto 50000 en el servidor remoto "**myserver**" como nodo "db2node", especifique el mandato siguiente desde una línea de mandatos de Db2

   db2 => CATALOG TCPIP NODE db2node REMOTE myserver SERVER 50000

Para obtener información más detallada sobre el nodo de catálogo, consulte https://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.client.doc/doc/t0005621.html

4. Si la estación de trabajo del Agente de Db2 es UNIX/Linux,
   - Cree un usuario con un nombre de nodo que se utilice en el mandato de catalogación

     Emita el mandato

     useradd -g <grupo> -m -d <dir_inicio> <usuario> -p <contraseña>

     donde

     – **<grupo>** representa un grupo para los propietarios de instancia de DB2 UDB.
     – **<usuario>** representa un **username** en la estación de trabajo de cliente. **username** debe coincidir con el nombre de nodo por el que la instancia de servidor se ha catalogado en el sistema de agente.
   - Compruebe el nombre de la instancia del cliente de Db2 en la que se cataloga la instancia de remota servidor de Db2 y asigne al propietario de esta instancia los permisos de lectura, escritura y ejecución del directorio de inicio del usuario que se acaba de crear. Este paso es necesario para que el entorno cliente de Db2 esté disponible para llevar a cabo operaciones en el nodo remoto
   - Emita el mandato

     chmod -R 775 /home/<nombre_nodo>

     donde

     – **<nombre_nodo>** representa un nombre de usuario local de la instancia de Db2 en el componente de cliente.
5. Catalogue todas las bases de datos que desee supervisar en la instancia de cliente que se halla en la estación de trabajo del Agente de Db2.

   Emita el mandato en el CLP de Db2 para catalogar la base de datos.

   CATALOG DATABASE <nombre_base_datos> AS <alias_base_datos> AT NODE <nombre_nodo>authentication server

   a. <nombre_base_datos> representa el nombre de la base de datos del servidor.
   b. <alias_base_datos> representa el apodo local de la base de datos en el cliente de Db2.
   c. <nombre_nodo> representa un apodo local de la instancia de Db2 en el componente de cliente en el que se ha catalogado la base de datos.

   Para catalogar una base de datos denominada "ejemplo" en un nodo de catálogo "nodo_db2" con el alias "dbAlias1", escriba el mandato siguiente desde el indicador de mandatos de Db2.

   db2 => CATALOG DATABASE ejemplo AS dbAlias1 AT NODE db2node authentication server

Configuración de la supervisión de Hadoop

Debe configurar el Monitoring Agent for Hadoop para que el agente pueda recopilar datos de un clúster Hadoop que supervisa. El agente puede supervisar un clúster Hadoop de nodo único y un clúster Hadoop de varios nodos.

Antes de empezar

Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Hadoop.

Asegúrese de que los siguientes hosts puedan resolverse desde el sistema en el que está instalado el Agente de Hadoop:

- Todos los hosts Hadoop que desea configurar, como por ejemplo NameNode, ResourceManager, etc.
- Los hosts Hadoop sólo con el rol NodeManager

Por ejemplo, puede seguir estos pasos para resolver los hosts:

- Añadir la dirección IP, el nombre de host y el nombre de dominio completo de todos los hosts Hadoop al archivo `hosts` que está disponible en la siguiente vía de acceso:
  - Windows `C:\Windows\System32\drivers\etc\hosts`
  - Linux AIX `/etc/hosts`
- Añadir el sistema en el que está instalado el Agente de Hadoop al mismo dominio que los hosts Hadoop.

Recuerde: Para supervisar un clúster de Hadoop que está protegido con autenticación basada en Kerberos SPNEGO, asegúrese de que los siguientes hosts puedan resolverse desde el sistema en el que está instalado el Agente de Hadoop.

Acerca de esta tarea

El Agente de Hadoop es un agente de instancia única. Debe configurar el agente manualmente una vez esté instalado. El Agente de Hadoop puede configurarse en sistemas Windows, Linux y AIX.

Recuerde:

- En un clúster Hadoop de nodo único, el mismo nodo desempeña todos los roles, como por ejemplo NameNode, ResourceManager y NameNode secundario, de acuerdo con la configuración del clúster Hadoop. Sin embargo, en un clúster Hadoop de varios nodos, diferentes nodos Hadoop desempeñan estos roles.
- Al configurar el agente, éste detecta automáticamente DataNodes y NodeManagers en el clúster Hadoop que se está supervisando.

Al actualizar desde el agente basado en socket (8.1.2 Fix Pack 2 o anterior) al agente basado en la API REST (8.1.3 o posterior), siga los pasos de configuración que se especifican en los temas subsiguientes. Sin embargo, asegúrese de especificar los nombres de host según las siguientes directrices cuando configure el agente.

- El nombre de host de diversos procesos de daemon (NameNode, ResourceManger, etc.) que especifique debe ser el mismo (mayúsculas/minúsculas y formato) que los nombres de host que están configurados para el agente basado en socket.
- Debe utilizarse el nombre de dominio completo (FQDN) al especificar un nombre de host. Por ejemplo, `hos1.ibm.com`. Si la longitud de FQDN supera los 25 caracteres, especifique sólo el nombre de host abreviado sin el nombre de dominio. Por ejemplo, si el FQDN de un host es *myhadoopclustersetupnode.ibm.com*, el nombre de host abreviado es `myhadoopclustersetupnode`.

Después de configurar el agente que se actualiza y ver los datos en la Consola de Cloud APM, revierta los cambios que se han realizado en el archivo `hadoop-metrics2.properties` para el Agente de Hadoop. Para obtener detalles, consulte “Actualización de los agentes” en la página 1173.

En sistemas Windows, puede ejecutar el Agente de Hadoop con un usuario no administrador. Sin embargo, dicho usuario requiere un permiso específico para ver datos de los paneles de instrumentos. Para obtener información sobre cómo otorgar este permiso, consulte “Otorgamiento de permiso a usuarios no administradores” en la página 272.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte “Historial de cambios” en la página 52.

Configuración del agente en sistemas Windows

Puede configurar el agente en sistemas Windows utilizando la ventana de **IBM Performance Management**.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en **Monitoring Agent for Hadoop**.
3. Pulse **Configurar agente**.

   Atención: Si **Configurar agente** está inhabilitado, pulse **Reconfigurar**.

   Se abre la ventana **Configurar Monitoring Agent for Hadoop**.
4. Para supervisar el clúster de Hadoop con la autenticación basada en Kerberos SPNEGO habilitada, siga estos pasos:
   a) Bajo **¿Está habilitada la autenticación basada en Kerberos SPNEGO para servicios de Hadoop basados en HTTP el clúster Hadoop?**, pulse **Sí**.

      Si tiene autenticación basada en Kerberos SPNEGO para proteger los puntos finales de REST de los servicios Hadoop basados en HTTP en el clúster de Hadoop, pulse **No** y a continuación los valores de los campos **Nombre de territorio**, **Nombre de host de KDC**, **Nombre de identificador individual de SPNEGO** y **Archivo de tabla de claves de SPNEGO** se pueden conservar en blanco.

   b) En el campo **Nombre de reino**, especifique el nombre del reino de Kerberos que se utiliza para crear principios de servicio.
      Normalmente, un nombre de reino coincide con el nombre de dominio. Por ejemplo, si el sistema está en el dominio `tivoli.ibm.com`, el nombre de reino de Kerberos es `TIVOLI.IBM.COM`. Este nombre es sensible a mayúsculas y minúsculas.

   c) En el campo **Nombre de host KDC**, especifique el nombre de dominio completo (FQDN) del host KDC (centro de distribución de claves) para el reino especificado.

      También puede especificar la dirección IP del host KDC en lugar del nombre del FQDN. En el caso del KDC de Active Directory, el controlador de dominio es el host KDC.

   d) En el campo **Nombre de identificador individual de SPNEGO**, especifique el nombre del principal de Kerberos utilizado para acceder a puntos finales de REST de servicios basados en HTTP autenticados mediante SPNEGO.

      El nombre es sensible a mayúsculas y minúsculas y el formato de nombre es HTTP/*nombre_host_completo*@*reino_kerberos*

   e) En el campo **Archivo de tabla de claves de SPNEGO** especifique el nombre del archivo de tabla de claves del servicio de SPNEGO con la vía de acceso completa o pulse **Examinar** y selecciónelo.

      El archivo de tabla de claves contiene los nombres de claves y principales de servicio de Kerberos. Este archivo proporciona acceso directo a servicios de Hadoop sin que sea necesaria una contraseña para cada servicio. El archivo se encuentra en la vía de acceso siguiente: `etc/security/keytabs/`
      Asegúrese de que el nombre principal de SPNEGO y el archivo de tabla de claves pertenecen al mismo host. Por ejemplo, si el nombre principal es *HTTP/abc.ibm.com@IBM.COM*, el archivo de tabla de claves que se utiliza debe pertenecer al host *abc.ibm.com*.
      Si el agente está instalado en un sistema remoto, copie el archivo de tabla de claves del principal en el sistema remoto en cualquier vía de acceso y a continuación especifique esta vía de acceso en el campo **Archivo de tabla de claves de SPNEGO**.

   f) Pulse **Siguiente**.
5. Para supervisar el clúster de Hadoop con HTTPS/SSL habilitado, siga estos pasos:
   a) En **Está habilitado el SSL de clúster de Hadoop**, pulse **Sí**

Si no desea que el clúster de Hadoop esté habilitado para SSL, seleccione **No** y los valores de los campos **Vía de acceso de archivo de almacén de confianza**, **Contraseña de almacén de confianza** se pueden mantener en blanco.

b) En **Vía de acceso de archivo de almacén de confianza**, seleccione el archivo Almacén de confianza almacenado en la máquina local.

Este archivo se puede copiar del clúster de Hadoop en la máquina local y luego se puede utilizar para la configuración.

c) En **Contraseña de almacén de confianza**, escriba la contraseña que ha creado al configurar el archivo Almacén de confianza.

6. Para especificar valores para los parámetros del clúster de Hadoop, siga estos pasos:

a) En el campo **Nombre exclusivo de clúster de Hadoop**, especifique el nombre exclusivo del clúster Hadoop que indica la versión y el tipo de Hadoop. El límite máximo de caracteres para este campo es 12.

b) En el campo **Nombre de host de NameNode**, especifique el nombre de host del nodo donde se ejecuta el proceso de daemon de NameNode.

c) En el campo **Puerto de NameNode**, especifique el número de puerto asociado con el proceso de daemon del NameNode. El número de puerto predeterminado es 50070.

d) En el campo **Nombre de host de ResourceManager**, especifique el nombre de host del nodo donde se ejecuta el proceso de daemon de ResourceManager.

e) En el campo **Puerto de ResourceManager**, especifique el número de puerto asociado con el proceso de daemon del ResourceManager. El número de puerto predeterminado es 8088.

f) Opcional: En el campo **Nombre de host de JobHistoryServer**, especifique el nombre de host del nodo donde se ejecuta el proceso de daemon de JobHistoryServer.

g) Opcional: En el campo **Puerto de JobHistoryServer**, especifique el número de puerto asociado con el proceso de daemon del JobHistoryServer. El número de puerto predeterminado es 19888.

h) Opcional: En el campo **Nombre de host de NameNode adicional**, especifique el nombre de host donde se ejecuta el proceso de daemon de un NameNode en espera (Standby) o NameNode secundario (Secondary).

i) Opcional: En el campo **Puerto de NameNode adicional**, especifique el número de puerto asociado con el proceso de daemon de un NameNode en espera o de un NameNode secundario.

Recuerde: Si el NameNode adicional es un NameNode en espera, el número de puerto predeterminado que está asociado con el proceso de daemon del NameNode en espera es el 50070. Si el NameNode adicional es un NameNode secundario, el número de puerto predeterminado que está asociado con el proceso de daemon del NameNode secundario es el 50090.

j) Pulse **Probar conexión** para verificar la conexión con los nombres de host y puertos especificados.

Después de pulsar **Probar conexión**, se visualizará un mensaje de validación adecuada cuando:

- La conexión a los nombres de host y puertos especificados se haya establecido o haya fallado.
- Un valor para un nombre de host se haya dejado en blanco.
- Un valor para un puerto se haya dejado en blanco.
- Se haya especificado un valor no entero para un número de puerto.

Actualice los valores de configuración según lo indicado en los mensajes de validación y verifique la conexión nuevamente.

k) Opcional: Para añadir ResourceManagers en espera al clúster Hadoop, pulse **Sí** en **ResourceManager(s) en espera en clúster Hadoop**.

Posteriormente se le solicitará que añada los detalles de Detalles de ResourceManagers en espera.

l) Opcional: Para supervisar servicios de Hadoop en el clúster de Hadoop gestionado por Apache Ambari, pulse **Sí** bajo **Supervisión de servicios de Hadoop para instalaciones Hadoop basadas en Ambari** y a continuación pulse **Siguiente**.

7. Opcional: Para especificar los detalles del servidor Ambari para supervisar servicios de Hadoop, siga estos pasos:
   a) En el campo **Nombre de host de servidor Ambari**, especifique el nombre de host en el que se ejecuta el servidor Ambari.
   b) En el campo **Puerto del servidor Ambari** especifique el número de puerto asociado con el servidor Ambari.
   El número de puerto predeterminado es 8080.
   c) En el campo **Nombre de usuario de Ambari** especifique el nombre del usuario de Ambari.
   d) En el campo **Contraseña de usuario de Ambari**, especifique la contraseña del usuario de Ambari.
   e) Pulse **Siguiente**.
8. Para especificar valores de los parámetros de Java, siga estos pasos:
   a) En la lista **Nivel de rastreo de Java**, seleccione un valor para el nivel de rastreo utilizado por los proveedores de Java.
   b) Opcional: En el campo **Argumentos de JVM**, especifique una lista de argumentos para la máquina virtual Java.
   La lista de argumentos debe ser compatible con la versión de Java que se instala junto con el agente.
   c) Pulse **Siguiente**.
9. Opcional: Para añadir ResourceManagers en espera, siga estos pasos:
   a) Pulse **Nuevo**.
   b) En el campo **Nombre de host de ResourceManager en espera**, especifique el nombre de host del nodo donde se ejecuta el proceso de daemon de ResourceManager en espera.
   c) En el campo **Puerto de ResourceManager en espera**, especifique el número de puerto asociado con el proceso de daemon del ResourceManager en espera. El número de puerto predeterminado es 8088.
   d) Pulse **Probar conexión** para validar la conexión con el nombre de host y el número de puerto especificados.
   Después de pulsar **Probar conexión**, se visualizará un mensaje de validación adecuada cuando:
   - La conexión a los nombres de host y puertos especificados se haya establecido o haya fallado.
   - Un valor para un nombre de host se haya dejado en blanco.
   - Un valor para un puerto se haya dejado en blanco.
   - Se haya especificado un valor no entero para un número de puerto.

   Actualice los valores de configuración según lo indicado en los mensajes de validación y verifique la conexión nuevamente.
   e) Repita los pasos a, b y c para añadir más ResourceManagers en espera.
   Si desea eliminar alguno de los ResourceManagers en espera, pulse **Suprimir** para el ResourceManager en espera que desea eliminar.
   f) Pulse **Siguiente**.
10. En el campo **Vía de acceso de clases para los jar externos**, especifique la vía de acceso de clases los archivos JAR.
    Esta vía de acceso de clases se añade a la vía de acceso de clases generada por el agente. Puede dejar este campo en blanco.
11. Pulse **Aceptar**.
    Los valores de configuración especificados se guardarán.
12. Pulse el botón derecho del ratón en **Monitoring Agent for Hadoop** y pulse **Iniciar**.

Qué hacer a continuación

1. Habilite los sucesos de subnodo para ver umbrales de sucesos del Agente de Hadoop. Para obtener más información acerca de la habilitación de sucesos de subnodo, consulte "Configuración del panel de instrumentos para visualizar sucesos Hadoop" en la página 272.
2. Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del agente en sistemas Linux y AIX

Ejecute el script de configuración y responda a las solicitudes para configurar el agente en sistemas Linux y AIX.

Procedimiento

1. En la línea de mandatos, ejecute el mandato siguiente: *dir_instalación*/bin/hadoop-agent.sh config
   Donde *dir_instalación* es el directorio de instalación del agente de Hadoop.
   El agente se instala en el directorio de instalación predeterminado: /opt/ibm/apm/agent
2. Cuando la línea de mandatos muestre el siguiente mensaje, escriba 1 para continuar con los pasos de configuración y pulse Intro.
   ¿Desea editar el valor "Monitoring Agent for Hadoop"? [1= Sí, 2= No]
3. Cuando la línea de mandatos muestre el siguiente mensaje, escriba 1 para especificar valores para supervisar el clúster de Hadoop con la autenticación basada en Kerberos SPNEGO habilitada y pulse Intro. De lo contrario, escriba 2 y pulse Intro y podrá conservar un valor en blanco para los campos **Nombre de territorio**, **Nombre de host de KDC**, **Nombre de identificador individual de SPNEGO** y **Archivo de tabla de claves de SPNEGO**:
   Está habilitada la autenticación basada en Kerberos SPNEGO para los servicios de Hadoop basados en HTTP en el clúster de Hadoop\: [1=Sí, 2=No (el valor predeterminado es 2)
   a) Para el parámetro **Nombre de territorio**, especifique el nombre del reino de Kerberos que se utiliza para crear principales de servicio.
   Normalmente, un nombre de reino coincide con el nombre de dominio. Por ejemplo, si el sistema está en el dominio tivoli.ibm.com, el nombre de reino de Kerberos es TIVOLI.IBM.COM. Este nombre es sensible a las mayúsculas y minúsculas.
   b) En el campo **Nombre de host KDC**, especifique el nombre de dominio completo (FQDN) del host KDC (centro de distribución de claves) para el reino especificado. También puede especificar la dirección IP del host KDC en lugar del nombre del FQDN. En el caso del KDC de Active Directory, el controlador de dominio es el host KDC
   c) Para el parámetro **Nombre de identificador individual de SPNEGO**, especifique el nombre del principal de Kerberos utilizado para acceder a puntos finales de REST de servicios basados en HTTP autenticados mediante SPNEGO.
   El nombre es sensible a mayúsculas y minúsculas y el formato de nombre es HTTP/*nombre_host_completo*@*reino_kerberos*
   d) Para el parámetro **Archivo de tabla de claves de SPNEGO**, especifique el nombre del archivo de tabla de claves del servicio SPNEGO con la vía de acceso completa.
   El archivo de tabla de claves contiene los nombres de claves y principales de servicio de Kerberos. Este archivo proporciona acceso directo a servicios de Hadoop sin que sea necesaria una contraseña para cada servicio. El archivo se encuentra en la vía de acceso siguiente: etc/security/keytabs/
   Asegúrese de que el nombre principal de SPNEGO y el archivo de tabla de claves pertenecen al mismo host. Por ejemplo, si el nombre principal es *HTTP/abc.ibm.com@IBM.COM*, el archivo de tabla de claves que se utiliza debe pertenecer al host *abc.ibm.com*.

Si el agente está instalado en un sistema remoto, copie el archivo de tabla de claves del principal en el sistema remoto en cualquier vía de acceso y a continuación especifique esta vía de acceso para el parámetro **Archivo de tabla de claves de SPNEGO**.

4. Cuando la línea de mandatos muestre el siguiente mensaje, escriba 1 para especificar los valores para supervisar el clúster de Hadoop con SSL habilitado y pulse **Intro**. De lo contrario, escriba 2 y pulse **Intro** y podrá conservar un valor en blanco para los campos **Vía de acceso de archivo de almacén de confianza** y **Contraseña de almacén de confianza**:
   `Está habilitado el SSL de clúster de Hadoop [ 1=Sí, 2=No (el valor predeterminado es: 2)`
   a) En **Vía de acceso de archivo de almacén de confianza**, especifique la vía de acceso del archivo Almacén de confianza almacenado en la máquina local.

      Este archivo se puede copiar del clúster de Hadoop en la máquina local y luego se puede utilizar para la configuración.

   b) En **Contraseña de almacén de confianza**, especifique la contraseña que ha creado al configurar el archivo Almacén de confianza.
5. Cuando se le solicite especificar los detalles del clúster de Hadoop, especifique un valor adecuado para cada uno de los parámetros siguientes y pulse Intro.
   a) En el **Nombre exclusivo de clúster de Hadoop**, especifique el nombre exclusivo del clúster Hadoop que indica la versión y el tipo de Hadoop. El límite máximo de caracteres para este campo es 12.

   b) En el parámetro **Nombre de host de NameNode**, especifique el nombre de host del nodo donde se ejecuta el proceso de daemon de NameNode y pulse Intro.

      Atención: Si pulsa Intro sin especificar un nombre de host, se le solicitará que especifique el nombre de host.

   c) En el parámetro **Puerto de NameNode**, especifique el número de puerto asociado con el proceso de daemon del NameNode y pulse Intro. El número de puerto predeterminado es 50070.

   d) En el parámetro **Nombre de host de ResourceManager**, especifique el nombre de host del nodo donde se ejecuta el proceso de daemon de ResourceManager y pulse Intro.

      Atención: Si pulsa Intro sin especificar un nombre de host, se le solicitará que especifique el nombre de host.

   e) En el parámetro **Puerto de ResourceManager**, especifique el número de puerto asociado con el proceso de daemon del ResourceManager. El número de puerto predeterminado es 8088.
6. Opcional: Cuando se le solicite especificar los detalles de los parámetros siguientes del clúster de Hadoop, acepte el valor predeterminado o especifique un valor adecuado para cada uno de los parámetros siguientes y pulse Intro:
   a) En el parámetro **Nombre de host de JobHistoryServer**, especifique el nombre de host del nodo donde se ejecuta el proceso de daemon de JobHistoryServer.

   b) En el parámetro **Puerto de JobHistoryServer**, especifique el número de puerto asociado con el proceso de daemon del JobHistoryServer. El número de puerto predeterminado es 19888.

   c) En el parámetro **Nombre de host de NameNode adicional**, especifique el nombre de host del nodo donde se ejecuta el proceso de daemon de un NameNode secundario o en espera.

   d) En el parámetro **Puerto de NameNode adicional**, especifique el número de puerto asociado con el proceso de daemon de un NameNode secundario o en espera. El número de puerto predeterminado para un NameNode secundario es 50090. Por un NameNode en espera, el número de puerto predeterminado es 50070.
7. Opcional: Cuando la línea de mandatos muestre el siguiente mensaje, especifique 1 para añadir detalles de ResourceMangers en espera para el clúster de alta disponibilidad y pulse Intro.
   `ResourceManager(s) en espera en clúster Hadoop [ 1=Sí, 2=No ] (el valor predeterminado es 2):`
8. Cuando la línea de mandatos visualiza el mensaje siguiente, especifique 1 y pulse Intro para supervisar servicios de Hadoop en el clúster de Hadoop gestionado por Ambari:

`Supervisión de servicios de Hadoop para instalaciones Hadoop basadas en Ambari [ 1=Sí, 2=No ] (el valor predeterminado es: 2):`
De lo contrario, retenga el valor predeterminado de 2 y pulse Intro. Si permite la supervisión de los servicios de Hadoop, especifique un valor para cada uno de los parámetros siguientes del servidor Ambari y pulse Intro:

a) Para el parámetro **Nombre de host de servidor Ambari**, especifique el nombre de host en el que se ejecuta el servidor Ambari.

b) Para el parámetro **Puerto del servidor Ambari**, especifique el número de puerto asociado con el servidor Ambari.
El número de puerto predeterminado es 8080.

c) Para el parámetro **Nombre de usuario de Ambari** especifique el nombre del usuario de Ambari.

d) Para el parámetro **Contraseña de usuario de Ambari** especifique la contraseña del usuario de Ambari.

9. Cuando la línea de mandatos muestre el siguiente mensaje, seleccione el nivel de rastreo Java adecuado y pulse Intro:
`Este parámetro le permite especificar el nivel de rastreo utilizado por los proveedores de Java Nivel de rastreo de Java [ 1=Desactivado, 2=Error, 3=Aviso, 4=Información, 5=Depuración mínima, 6=Depuración media, 7=Depuración máxima, 8=Todo ] (el valor predeterminado es: 2)`
10. Opcional: Cuando la línea de mandatos muestre el siguiente mensaje, especifique los argumentos para la máquina virtual Java y pulse Intro. La lista de argumentos debe ser compatible con la versión de Java que se instala junto con el agente.
`Este parámetro permite especificar una lista opcional de argumentos para la Java Virtual Machine Argumentos de JVM (el valor predeterminado es:)`
11. Opcional: Cuando la línea de mandatos muestre el siguiente mensaje, especifique 1 para añadir los detalles siguientes de ResourceManagers en espera y pulse Intro:
`Editar valores de "Clúster de alta disponibilidad (HA) Hadoop con ResourceManagers en espera", [1=Añadir, 2=Editar, 3=Supr, 4=Siguiente, 5=Salir] (el valor predeterminado es: 5): 1`

a) En el parámetro **`Nombre de host de ResourceManager en espera`**, especifique el nombre de host del nodo donde se ejecuta el proceso de daemon del ResourceManager en espera.

b) En **`Puerto de ResourceManager en espera`**, especifique el número de puerto asociado con el proceso de daemon del ResourceManager en espera. El número de puerto predeterminado es 8088.

c) Cuando se le solicite, especifique 1 para añadir más ResourceManagers en espera y repita los pasos a y b, o especifique 5 para ir al paso siguiente.

- Para editar los valores de configuración de un determinado ResourceManager en espera, especifique 4 y pulse Intro hasta que vea el nombre de host del ResourceManager en espera necesario.
- Para eliminar un ResourceManager en espera, especifique 3 y pulse Intro después de ver el nombre de host del ResourceManger en espera que desea eliminar.

12. Cuando se le solicite, especifique la vía de acceso de clases para los archivos JAR necesarios para el proveedor de datos de la API Java y pulse Intro.
Los valores de configuración especificados se guardarán y se visualizará un mensaje de confirmación.
13. Ejecute el mandato siguiente para iniciar el agente:*dir_instalación*`/bin/hadoop-agent.sh start`

Qué hacer a continuación

1. Habilite los sucesos de subnodo para ver umbrales de sucesos del Agente de Hadoop. Para obtener más información acerca de la habilitación de sucesos de subnodo, consulte "Configuración del panel de instrumentos para visualizar sucesos Hadoop" en la página 272.

2. Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Para algunos parámetros, los valores predeterminados se proporcionan entre caracteres de comentario. Puede especificar diferentes valores para estos parámetros y eliminar los códigos de comentario colocados al principio de los parámetros.

Acerca de esta tarea

Puede utilizar el archivo de respuestas silencioso para configurar el Agente de Hadoop en sistemas Linux, AIX y Windows.

Procedimiento

1. Abra el archivo de respuestas silencioso que está disponible en esta vía de acceso: *dir_instalación*\samples\hadoop_silent_config.txt.
2. En el archivo de respuestas, complete estos pasos:
   a) Cuando desee supervisar el clúster de Hadoop habilitado para la autenticación basada en Kerberos SPNEGO, especifique `sí` y especifique valores para los parámetros siguientes:

   ```
   HADOOP_REALM_NAME
   HADOOP_KDC_HOSTNAME
   HADOOP_PRINCIPAL_NAME
   HADOOP_SPNEGO_KEYTAB
   ```

   b) Cuando desee supervisar el clúster de Hadoop que está habilitado para SSL, escriba `yes` y escriba los valores para los siguientes parámetros:

   ```
   HADOOP_TRUSTSTORE_PATH
   HADOOP_TRUSTSTORE_PASSWORD
   ```

   c) Especifique valores para los parámetros siguientes de clúster: NameNode (NN), ResourceManager (RM) y Job History Server (JHS):

   ```
   HADOOP_CLUSTER_NAME (opcional)
   HADOOP_NN_HOSTNAME
   HADOOP_NN_PORT
   HADOOP_RM_HOSTNAME
   HADOOP_RM_PORT
   HADOOP_JHS_HOSTNAME
   (opcional)
   HADOOP_JHS_PORT (opcional)
   ```

   d) Opcional: Para el parámetro **HADOOP_ADDITIONAL_NN_HOSTNAME**, especifique el nombre de host del NameNode Standby (en espera) o Secondary (secundario).
   e) Opcional: Para el parámetro **HADOOP_ADDITIONAL_NN_PORT**, especifique el número de puerto del NameNode Standby (en espera) o Secondary (secundario).

   Recuerde: Si el NameNode adicional es un NameNode en espera, el número de puerto predeterminado que está asociado con el proceso de daemon del NameNode en espera es el 50070. Si el NameNode adicional es un NameNode secundario, el número de puerto predeterminado que está asociado con el proceso de daemon del NameNode secundario es el 50090.

   f) Opcional: Para el parámetro **Hadoop_SRM**, especifique `Yes` para añadir ResourceManagers Standby para un clúster de alta disponibilidad, y vaya al paso g.
   g) Opcional: Para supervisar servicios de Hadoop en el clúster de Hadoop gestionado por Ambari, especifique valores para cada uno de los parámetros siguientes y pulse Intro:

   ```
   AMBARI_SERVER_HOSTNAME
   AMBARI_SERVER_PORT
   ```

```
USERNAME_OF_AMBARI_USER
PASSWORD_OF_AMBARI_USER
```

h) Para el parámetro **JAVA_TRACE_LEVEL**, especifique el nivel de rastreo adecuado.

i) Opcional: Para el parámetro **JAVA_JVM_ARGS**, especifique argumentos para la máquina virtual Java™.

j) Opcional: Añada el nombre de host y el número de puerto de un ResourceManager en espera en el formato siguiente: HADOOP_SRM_PORT.*hadoop_srm_config_sec_1*=8088

Donde *hadoop_srm_config_sec_1* es el nombre de host del nodo en el que se ejecuta el proceso de daemon para ResourceManager en espera, y 8088 es el número de puerto predeterminado. Para añadir más ResourceManagers en espera, añada el nombre de host y el número de puerto de otros ResourceManagers en espera en nuevas líneas en el mismo formato.

3. Guarde el archivo de respuestas y ejecute el mandato siguiente:

Linux AIX *dir_instalación*/bin/hadoop-agent.sh config *dir_instalación*/samples/hadoop_silent_config.txt

Windows *dir_instalación*\bin\hadoop-agent.bat config *dir_instalación*\samples\hadoop_silent_config.txt

4. Inicie el agente:

Linux AIX Ejecute el mandato siguiente: *dir_instalación*\bin\hadoop-agent.sh start

Windows Pulse el botón derecho del ratón en **Monitoring Agent for Hadoop** y, a continuación, pulse **Iniciar**.

Qué hacer a continuación

1. Habilite los sucesos de subnodo para ver umbrales de sucesos del Agente de Hadoop. Para obtener más información acerca de la habilitación de sucesos de subnodo, consulte "Configuración del panel de instrumentos para visualizar sucesos Hadoop" en la página 272.
2. Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del panel de instrumentos para visualizar sucesos Hadoop

Debe configurar el panel de instrumentos para habilitar los sucesos de subnodo de forma que la pestaña **Sucesos** pueda visualizar sucesos Hadoop.

Acerca de esta tarea

El valor predeterminado de **Habilitar sucesos de subnodo** es falso. Cambie este valor a verdadero para visualizar sucesos Hadoop.

Procedimiento

1. Abra la Consola de Cloud APM y vaya a **Configuración del sistema**.
2. En la página **Configuración avanzada**, pulse **Integración de interfaz de usuario** bajo **Categorías de configuración**.
3. En la lista **Habilitar sucesos de subnodo**, seleccione **True**.
4. Pulse **Guardar**.

Otorgamiento de permiso a usuarios no administradores

En sistemas Windows, otorgue el permiso *Depurar programa* a un usuario no administrador para ejecutar el Agente de Hadoop. Este permiso es necesario para ver datos de los paneles de instrumentos del Agente de Hadoop.

Procedimiento

Complete los pasos siguientes en el sistema donde está instalando el agente de Hadoop:

1. Pulse **Inicio > Panel de control > Herramientas administrativas**.
2. Efectúe una doble pulsación en **Política de seguridad local**.
3. En el panel Valores de seguridad, expanda **Políticas locales** y pulse **Asignación de derechos de usuario**.
4. Pulse con el botón derecho del ratón **Depurar programas** y pulse **Propiedades**.
5. Pulse **Añadir usuario o grupo** y añada el nombre del usuario no administrador al que desea otorgar este permiso.
6. Pulse **Aceptar**.

Qué hacer a continuación

Configure y ejecute el Agente de Hadoop con el usuario no administrador.

Configuración de la supervisión de HMC Base

Monitoring Agent for HMC Base proporciona la capacidad de supervisar la consola de gestión de hardware (HMC). El agente supervisa la disponibilidad y el estado de los recursos de HMC: CPU, memoria, almacenamiento y red. El agente también informa del inventario de HMC y la configuración de servidores Power, agrupaciones de CPU y LPARs. La utilización de CPU de los servidores Power, las LPARs y las agrupaciones se supervisa mediante los datos de muestra de rendimiento de la HMC.

Antes de empezar

Antes de configurar el Agente de HMC Base, debe realizar las tareas siguientes:

- Configure la conexión SSH entre el sistema que ejecuta el agente y HMC. Para obtener más información, consulte "Configuración de la conexión SSH" en la página 275.
- Prepare el SDK de HMC antes de iniciar la primera instancia de agente. Para obtener más información, consulte "Preparación del SDK para HMC" en la página 276.

Procedimiento

- Para configurar el agente mediante la edición del archivo de respuestas silenciosas y la ejecución del script sin interacción, siga estos pasos:
  1. Abra el archivo `hmc_base_silent_config.txt` en un editor de texto:
     - AIX *dir_instalación*`/samples/hmc_base_silent_config.txt`.
  2. Para **`Nombre de host HMC`**, puede especificar la dirección IP o el nombre de host.
  3. Para **`Nombre de usuario HMC`**, debe especificar el nombre de usuario de inicio de sesión para HMC, por ejemplo, **`HMC_USERNAME=`** *hscroot*.

     Nota: El nombre de usuario de inicio de sesión que asigna a HMC necesita autorización hscviewer como mínimo.
  4. Para **`Contraseña de HMC`**, debe especificar la contraseña del usuario.
  5. Para **`Número máximo de archivos de registro de proveedor de datos:`**, debe especificar el número máximo de archivos de registro de proveedor de datos creados. Por ejemplo, **`KPH_LOG_FILE_MAX_COUNT=`***10*.
  6. Para **`Tamaño máximo en KB de cada registro de proveedor de datos`**, debe especificar el tamaño máximo en KB que un archivo de registro de proveedor de datos puede alcanzar antes de crear un archivo de registro de datos, por ejemplo, **`KPH_LOG_FILE_MAX_SIZE=`** *5190*.

7. Para **Nivel de detalle en registro de proveedor de datos**, debe especificar la cantidad de detalle que el proveedor de datos incluye en los archivos de registro de proveedor, por ejemplo **KPH_LOG_LEVEL=***Fine*. Debe especificar uno de los valores siguientes:
   - 1= Off
   - 2=Severe
   - 3=Warning
   - 4=Info
   - 5=Fine
   - 6=Finer
   - 7=Finest
   - 8=All

   Importante: El valor predeterminado es 4.
8. Guarde y cierre el archivo `hmc_base_silent_config.txt` y especifique `./hmc_base-agent.sh config` *`nombre_instancia dir_instal`*`/samples/hmc_base_silent_config.txt` donde *nombre_instancia* es el nombre que desea dar a la instancia y *dir_instal* es el directorio de instalación de Agente de HMC Base. El directorio de instalación predeterminado es `/opt/ibm/apm/agent`.

- AIX Para configurar el agente mediante respuestas a las solicitudes, siga estos pasos:

1. Abra el directorio *`dir_instalación`*`/bin`, donde *dir_instalación* es el directorio de instalación del Agente de HMC Base.
2. Para configurar el Agente de HMC Base, ejecute el mandato siguiente: **./hmc_base-agent.sh config nombre_instancia**.
3. Cuando se le solicite **editar los valores de Monitoring Agent for HMC Base**, pulse **Intro**. El valor predeterminado es Sí.
4. Para especificar la información de configuración de HMC, realice los pasos siguientes.
   a. Cuando se le solicite el **Nombre de host HMC**, escriba el nombre de host o la dirección IP y pulse **Intro**.
   b. Cuando se le solicite el **Nombre de usuario HMC**, teclee el nombre de usuario de inicio de sesión asociado a HMC y pulse **Intro**.
5. Cuando se le solicite la **Contraseña de HMC**, escriba la contraseña del usuario.
6. Para especificar la información de proveedor de datos, realice los pasos siguientes:
   a. Cuando se le solicite el **número máximo de archivos de registro de proveedor de datos**, teclee la cantidad de archivos de registro y pulse **Intro**.

      El número máximo de archivos de registro de proveedor predeterminado es 10.
   b. Cuando se le solicite el **tamaño máximo en KB de cada registro de proveedor de datos**, teclee el tamaño y pulse **Intro**.

      El tamaño máximo predeterminado en KB es 5190.
   c. Cuando se le solicite el **Nivel de detalle en registro de proveedor de datos**, teclee uno de los niveles siguientes y pulse **Intro**:
      - 1= Off
      - 2=Severe
      - 3=Warning
      - 4=Info
      - 5=Fine
      - 6=Finer
      - 7=Finest

– 8=All

Qué hacer a continuación

- Para iniciar el agente, especifique: `./hmc_base-agent.sh start` *`nombre_instancia`*.
- Configure el servidor de consola HMC según las instrucciones en "Configuración del servidor de consola HMC para supervisión de E/S virtual" en la página 277 para supervisión de entrada/salida virtual.
- Habilite la supervisión de utilización de CPU y memoria según las instrucciones en "Habilitación de la supervisión de utilización de CPU y memoria" en la página 278.

Configuración de la conexión SSH

Debe configurar la conexión SSH entre el sistema que ejecuta el agente y la HMC para que el agente recopile datos.

Acerca de esta tarea

El proveedor de datos de agente recopila datos de la consola de gestión ejecutando mandatos CLI por SSH. De forma predeterminada, el proveedor de datos espera hasta 1 minuto a que un mandato CLI finalice la ejecución. Después de este tiempo, el proveedor de datos cierra la sesión SSH en la que se está ejecutando el mandato CLI, y ninguno de los datos para ese mandato está disponible en conjuntos de datos de agente hasta que el mandato se ejecuta satisfactoriamente. La vía de acceso predeterminada para el mandato SSH es `/usr/bin/ssh`. Si ha instalado SSH en una ubicación diferente, debe indicar la vía de acceso utilizando la variable de entorno **KPH_SSH_PATH**.

Procedimiento

Utilice uno de los métodos siguientes para configurar la conexión SSH.

- Utilice el script `setup_hmc_key.pl` para configurar la conexión SSH.
  a) Inicie la sesión en el servidor en el que está instalado el agente.
  b) Abra el directorio `dir_instal/aix526/ph/bin`, donde `dir_instal` es el directorio de instalación del Agente de HMC Base.
  c) Ejecute el mandato `perl setup_hmc_key.pl`.
  d) Responda a solicitudes y proporcione el nombre de host o dirección IP de la HMC; el nombre de usuario de la HMC, que debe tener autoridad equivalente a `hscviewer`; y la contraseña para crear el par de claves.
  e) Después de crear el par de claves, pruebe la conectividad ejecutando un mandato, por ejemplo, `ssh hscroot@hmchost lshmc -V`.
  Si SSH se conecta a esta HMC por primera vez, añada la HMC al archivo `ssh known_hosts` respondiendo con `yes` al mensaje siguiente:

```
No se puede establecer la autenticidad de host 'hmchost (3.3.333.333)'.
Huella dactilar de clave RSA es 4c:b4:26:27:38:f3:ec:58:01:92:26:f9:61:32:bb:4d.
¿Está seguro de que desea continuar la conexión (sí/no)? sí

Aviso: añadido permanentemente 'hmchost,3.3.333.333' (RSA) a la lista de hosts conocidos.
```

  El agente puede ahora utilizar SSH para recopilar datos de la HMC.
- Utilice el programa de utilidad `ssh-keygen` para generar claves y configurar la conexión SSH.
  a) Inicie la sesión en el servidor en el que está instalado el agente.
  b) Utilice el programa de utilidad `ssh-keygen` para generar claves públicas y privadas sin frase de contraseña.
  Por ejemplo, el mandato siguiente genera un conjunto de claves públicas y privadas:

```
ssh-keygen -t rsa -f /.ssh/id-rsa
```

Pulse Intro cuando se le solicite una frase de contraseña. La clave pública que se genera se almacena en el archivo /.ssh/id-rsa.pub. La clave privada se almacena en el archivo /.ssh/id-rsa.

c) Transfiera el archivo que contiene la clave pública al sistema de la HMC utilizando programas de utilidad como scp.

d) En el sistema de la HMC, añada el archivo de clave pública a la colección de claves almacenadas en la HMC.

Las claves almacenadas están en el archivo /.ssh/authorized_keys2.

e) Añada el nombre de host y la clave para la HMC en el archivo known_hosts.

Este archivo está en el directorio /.ssh.

a. Ejecute el mandato ssh "user"@"hmc_hostname" -i "private_keyfile" date.

b. Especifique sí cuando se le solicite almacenar las claves en caché. Este mandato añade la entrada al archivo known_hosts para conexiones futuras.

f) Ejecute el mandato ssh "user"@"hmc_hostname" date.

Si la fecha se devuelve sin solicitud de contraseña, significa que las claves SSH se han configurado satisfactoriamente.

Preparación del SDK para HMC

Debe preparar el SDK para HMC antes de iniciar la instancia de agente por primera vez.

Acerca de esta tarea

Antes de iniciar la primera instancia de agente, debe preparar la versión correspondiente del SDK para su HMC. Una vez completada la preparación, no será necesario repetir esta tarea para otras instancias de Agente de HMC Base que cree para el HMC de la misma versión. Para supervisar otra versión de HMC, repita estas tareas para volver a preparar el SDK.

Procedimiento

- En el directorio *dir_agente*/aix526/ph/bin ejecute la herramienta de script **prepareSDK.sh** para preparar automáticamente el SDK de HMC.
  - Si ve el mensaje SDK está preparado para HMC, la preparación se ha completado.
  - Si no ve el mensaje SDK está preparado para HMC, puede preparar manualmente el SDK para HMC.

    Para HMC V8.5.0, siga estos pasos:

    1. Utilice un navegador para descargar el SDK de HMC directamente con el URL siguiente:

       ```
       https://IP_HMC:12443/rest/api/web/sdk
       ```

       Cuando se le solicite, especifique el nombre de usuario y la contraseña de la cuenta hscroot. El nombre de archivo SDK tiene el formato pmc_sdk_*.zip.
    2. . Desempaquete el archivo zip del SDK y vaya al directorio IBM HMC REST Web Services SDK Runtime/lib/ibm3.
    3. Si todavía no existe, cree un subdirectorio <dir_agente>/aix526/ph/lib/*mi_versión_hmc*, donde *mi_versión_hmc* es la versión del entorno HMC, por ejemplo, 8502. Para determinar la versión del entorno HMC, ejecute el siguiente mandato:

       ```
       ssh hscroot@<HMC_IP> 'lshmc -v' | grep RM |
       awk -FR '{print $3}' | tr -d '.'
       ```

    4. Copie todos los archivos .jar de la carpeta IBM HMC REST Web Services SDK Runtime/lib/ibm3 del SDK de HMC en el directorio *dir_agente*/aix526/ph/lib/*versión_HMC*.

Para HMC V8.6.0 o V8.7.0, siga estos pasos:

1. Utilice un navegador para descargar el SDK de HMC directamente con el URL siguiente:

   ```
   https://IP_HMC:12443/rest/api/web/sdk
   ```

   Cuando se le solicite, especifique el nombre de usuario y la contraseña de la cuenta `hscroot`. El nombre de archivo SDK tiene el formato `pmc-rest-sdk*.zip`.
2. Desempaquete el archivo zip del SDK y vaya al subdirectorio `lib`.
3. Si todavía no existe, cree un subdirectorio `<dir_agente>/aix526/ph/lib/mi_versión_hmc`, donde *mi_versión_hmc* es la versión del entorno HMC, por ejemplo, 8602 o 87012. Para determinar la versión del entorno HMC, ejecute el siguiente mandato:

   ```
   ssh hscroot@<HMC_IP> 'lshmc -v' | grep RM |
   awk -FR '{print $3}' | tr -d '.'
   ```
4. Copie todos los archivos `.jar` de la carpeta `lib` del SDK de HMC en el directorio *dir_agente*`/aix526/ph/lib/`*mi_versión_hmc*.

Resultados
Ha preparado satisfactoriamente el SDK para HMC.

Qué hacer a continuación
Configure el Agente de HMC Base según las instrucciones del "Configuración de la supervisión de HMC Base" en la página 273.

Configuración del servidor de consola HMC para supervisión de E/S virtual

Antes de que el Agente de HMC Base pueda supervisar el estado de E/S virtual, debe configurar el servidor de consola HMC.

Procedimiento

Siga los pasos para configurar el servidor de consola HMC como requisitos previos para que el Agente de HMC Base pueda supervisar E/S virtual.

- Habilite la función PMC del servidor de consola HMC y de los servidores de E/S virtual.
  a) Inicie la sesión en el servidor de consola HMC utilizando el navegador en modalidad clásica.

     ```
     https://nombre_host_hmc
     ```

  b) Pulse **Gestión de HMC** > **Cambiar valores de Performance Monitoring**.

     Se visualiza la ventana **Cambiar valores de Performance Monitoring**.

  c) En la sección **Recopilación de datos de Performance Monitoring para gestionar servidores**, active la función **Recopilación** para los servidores correspondientes.

  d) Pulse en cada servidor de E/S virtual para mostrar la ventana **Propiedades de partición** para ese servidor.

  e) En la pestaña **General**, asegúrese de que el recuadro de selección de la opción **Permitir recopilación de información de rendimiento** está seleccionado.

     Pulse **Aceptar** para guardar los valores.

  Después de varios minutos, puede ver el tráfico de red y de almacenamiento de los servidores correspondiente en la página **Performance Monitoring**.
- Asegúrese de que el usuario HMC para el Agente de HMC Base tiene el privilegio correcto.
  a) Al añadir o editar el usuario, asegúrese de que el usuario tiene el rol **hmcviewer**, y que la opción **AllSystemResource** para este usuario está habilitada.

  b) En la ventana **Propiedades de usuario**, habilite la opción **Permitir acceso remoto a través de la web**.

Habilitación de la supervisión de utilización de CPU y memoria

Si la recopilación de datos de la utilización de CPU y memoria está inhabilitada, los datos de utilización de CPU y memoria de cada servidor de alimentación no aparecen en la interfaz de usuario.

Procedimiento

Utilice uno de los métodos siguientes para habilitar la supervisión de utilización de CPU y memoria.

- Habilite la supervisión de utilización de CPU y memoria ejecutando el siguiente mandato de gestión de HMC `chlparutil`.

  ```
  chlparutil-r config -m <nombreCEC> -s <la frecuencia de muestra en segundos, siempre 60>
  ```

- Habilite la supervisión de utilización de CPU y memoria en el servidor de consola HMC.
  a) Inicie la sesión en el servidor de consola HMC con modalidad clásica.
  b) Pulse el nodo **Servidores** en el árbol de navegación.
  c) Seleccione el servidor y vaya a **Operaciones** > **Datos de utilización** > **Cambiar la frecuencia de muestra**.
  d) Establezca una tasa de muestreo.
  La tasa de muestreo está inhabilitada de forma predeterminada. Puede establecer la tasa con valores adecuados, por ejemplo, `30 minutos`.

Configuración de la supervisión de HTTP Server

El Monitoring Agent for HTTP Server se inicia automáticamente después de la instalación. Para habilitar la recopilación de datos, asegúrese de que el servidor HTTP esté en ejecución y edite el archivo de configuración del servidor HTTP de modo que incluya una referencia al archivo de configuración del recopilador de datos del Agente de HTTP Server.

Antes de empezar

Hay dos archivos involucrados en la configuración del Agente de HTTP Server. Para ver ejemplos de estos archivos, consulte la sección Ejemplos. Localice y revise los archivos siguientes:

El archivo de configuración del recopilador de datos del Agente de HTTP Server

Después de instalar el Agente de HTTP Server, éste descubre el servidor HTTP y genera un archivo de configuración de recopilador de datos en el directorio *dir_instalación*/tmp/khu, donde *dir_instalación* es el directorio en el que está instalado el Agente de HTTP Server.

Si tiene varios servidores HTTP en el entorno, se genera un archivo de configuración de Agente de HTTP Server por cada servidor HTTP.

El nombre del archivo de configuración del Agente de HTTP Server se compone de dos partes y tiene el formato siguiente:

```
khu.vía de acceso completa del nombre de archivo de configuración de HTTP Server.conf
```

La primera parte del nombre del archivo de configuración del agente del agente es khu, siendo hu el código de agente del servidor HTTP.
La segunda parte del nombre del archivo de configuración del agente del agente se crea utilizando la vía de acceso completa y el nombre del archivo de configuración del agente del servidor HTTP, en la que / se sustituye por . . Por ejemplo, los nombres de archivo posibles son los siguientes:

Linux AIX `khu.usr.local.apache24.conf.httpd.conf`

Windows `khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf`

El archivo de configuración del recopilador de datos del Agente de HTTP Server contiene los elementos siguientes:

- Detalles sobre la vía de acceso del archivo httpd.conf que utiliza el servidor HTTP, por ejemplo, `KhuShmemPath "/IBM/HTTPServer/conf/httpd.conf"`.
- Ubicación de la biblioteca a cargar
- Permisos que están asociados con la memoria compartida

El archivo de configuración del servidor HTTP

Cada servidor HTTP tiene un archivo de configuración que, de forma predeterminada, se denomina *dir_instalación_servidor_http*`/conf/httpd.conf`, donde *dir_instalación_servidor_http* es el directorio donde se ha instalado el servidor HTTP. En algunos entornos, este nombre de archivo puede personalizarse. Compruebe el nombre de archivo exacto con el administrador del servidor HTTP.

Acerca de esta tarea

habilite el Agente de HTTP Server para la recopilación de datos en las situaciones siguientes:

- Después de instalar el Agente de HTTP Server
- Después de actualizar al Agente de HTTP Server versión 1.0.0.4, el nuevo alias provoca que los nodos del Agente de HTTP Server existentes queden fuera de línea en la Consola de Cloud APM.
- Después de actualizar desde la versión 1.0.0.4, los nodos del Agente de HTTP Server existentes pueden quedar fuera de línea en la Consola de Cloud APM. Esto puede ocurrir si tiene varias instancias de servidor HTTP con nombres de archivo de configuración del agente similares, por ejemplo, `httpd` y `httpd01`.

La herramienta de programa de utilidad de red de línea de mandatos netstat es necesaria para que el Agente de HTTP Server pueda descubrir correctamente el servidor HTTP en ejecución.

Importante: para resolver el problema de nodo de agente fuera de línea que se produce tras la actualización, debe añadir la nueva instancia del servidor HTTP en la Consola de Cloud APM después de completar esta tarea.

Procedimiento

1. Para activar la recopilación de datos, debe referenciar el archivo de configuración del recopilador de datos en el archivo de configuración del servidor HTTP mediante la sentencia `Include`. Añada la sentencia siguiente al final del archivo de configuración del servidor HTTP:

   ```
   Include "dir_instalación/tmp/khu/khu.vía de acceso completa del
   nombre de archivo de configuración de HTTP Server.conf"
   ```

   Por ejemplo,

   Linux AIX Si tiene un IBM HTTP Server que está instalado en el directorio `/opt/IBM/HTTPServer` y el archivo de configuración del recopilador de datos se encuentra en el directorio siguiente:

   ```
   /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
   ```

   Añada la sentencia siguiente al final del archivo de configuración del servidor HTTP `/opt/IBM/HTTPServer/conf/httpd.conf`:

   ```
   Include "/opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf"
   ```

   Windows Si tiene un IBM® HTTP Server que está instalado en el directorio `C:\ProgramFiles\IBM\HTTPServer` y el archivo de configuración del recopilador de datos se encuentra en el directorio siguiente:

   ```
   C:\IBM\APM\tmp\khu\khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf
   ```

Añada la sentencia siguiente al final del archivo de configuración del servidor HTTP `C:\Program Files\IBM\HTTPServer\conf\httpd.conf`:

```
Include "C:\IBM\APM\tmp\khu\khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf"
```

2. Cambie al siguiente directorio:

```
directorio_instalación_servidor_HTTP/bin
```

3. Reinicie el servidor HTTP. Por ejemplo:

Linux AIX

```
./apachectl -k stop
./apachectl -k start
```

Windows

```
httpd.exe -k stop
httpd.exe -k start
```

Resultados
Ha configurado satisfactoriamente el agente.

Qué hacer a continuación
Ahora, puede verificar que los datos del Agente de HTTP Server se visualizan en la consola de Cloud APM. Si desea instrucciones sobre cómo iniciar la consola de Cloud APM, consulte la sección Inicio de la consola de Cloud APM. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte Gestión de aplicaciones.

Nota: Si no hay tráfico en el servidor HTTP, no observará datos en la Consola de Cloud APM.

Módulo de Tiempo de respuesta de IBM HTTP Server

Si instala el agente de Supervisión de tiempo de respuesta para que funcione con el Módulo de Tiempo de respuesta de IBM HTTP Server, se supervisarán todos los puertos para solicitudes HTTP y HTTPS.

Módulo de Tiempo de respuesta de IBM HTTP Server
El Módulo de Tiempo de respuesta de IBM HTTP Server forma parte del Agente de HTTP Server. Si el Agente de HTTP Server se instala y configura antes o al mismo tiempo que el agente de Supervisión de tiempo de respuesta en Apache HTTP Server o IBM HTTP Server en AIX, Linux o Windows, el Módulo de Tiempo de respuesta de IBM HTTP Server se habilita automáticamente. Para obtener una descripción de la funcionalidad del Módulo de Tiempo de respuesta de IBM HTTP Server, consulte "Configuración del Módulo de Tiempo de respuesta de IBM HTTP Server" en la página 719.

Archivo de configuración del recopilador de datos
Después de instalar el Agente de HTTP Server, éste descubre el servidor HTTP y genera un archivo de configuración de recopilador de datos en el directorio *dir_instalación*/tmp/khu, donde *dir_instalación* es el directorio en el que está instalado el Agente de HTTP Server.

Para Apache HTTP Server, el archivo de configuración del recopilador de datos es:
`khu.usr.local.apache24.conf.httpd.conf`
Para IBM HTTP Server, el archivo de configuración del recopilador de datos es:
`khu.opt.IBM.HTTPServer.conf.httpd.conf`

Plug-ins
El Agente de HTTP Server está compuesto de dos plug-ins:

1. `khu_module` - este es el Agente de HTTP Server. Este plug-in es responsable de todos los paneles de instrumentos asociados con el Agente de HTTP Server. Para obtener más información, consulte la Referencia de Agente de HTTP Server.
2. `wrt_module` - este es el Módulo de Tiempo de respuesta de IBM HTTP Server

Estos dos plug-ins se indican en el archivo de configuración del recopilador de datos de la siguiente manera:

```
LoadModule khu_module

LoadModule wrt_module
```

Activar la recopilación de datos

Para activar la recopilación de datos, debe referenciar el archivo de configuración del recopilador de datos en el archivo de configuración del servidor HTTP mediante la sentencia `Include`. Añada la sentencia siguiente al final del archivo de configuración del servidor HTTP:

```
include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
```

Para obtener más información, consulte "Configuración de la supervisión de HTTP Server" en la página 278.

Una vez activada la recopilación de datos, se llenará el panel de instrumentos de usuario final.

Ejemplos de código del Agente de HTTP Server

Hay dos archivos involucrados en la configuración del Agente de HTTP Server. Son el archivo de configuración del recopilador de datos del Agente de HTTP Server y el archivo de configuración del servidor HTTP. También se suministra un ejemplo del archivo de correlaciones de alias de instancia como ayuda para explicar el funcionamiento del alias.

Ejemplos de archivo de recopilador de datos del Agente de HTTP Server

Para IBM HTTP Server versión 8 y posteriores de 64 bits, el archivo de configuración del recopilador de datos del Agente de HTTP Server contiene esta información:

```
#
# Valores para el módulo Monitoring Agent for HTTP Server.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache22dc_64.so"

<IfModule mod_khu.c>
   KhuShmemPerm 660
   KhuShmemPath "/opt/IBM/IHS/conf/httpd.conf"
   KhuCpsPath "/tmp/ihs/tmp/khu/khu_cps.properties"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  #Require all granted
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap22_64.so
WrtOriginID HU:tivvm09_httpd:HUS
```

Para IBM HTTP Server versión 7, de 32-bits, el archivo de configuración contiene esta información:

```
#
# Valores para el módulo Monitoring Agent for HTTP Server.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache22dc_32.so"

<IfModule mod_khu.c>
 KhuShmemPerm 660
 KhuShmemPath "/opt/IBM/HTTPServer/conf/httpd.conf"
 KhuCpsPath "/tmp/ihs/tmp/khu/khu_cps.properties"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
```

```
  Order deny,allow
  Allow from all
  #Require all granted
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap22.so
WrtOriginID HU:linux_httpd:HUS
```

Para Apache versión 2.4 de 64 bits, el archivo de configuración del Agente de HTTP Server contiene esta información:

```
#
# Valores para el módulo Monitoring Agent for HTTP Server.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache24dc_64.so"

<IfModule mod_khu.c>
 KhuShmemPerm 660
 KhuShmemPath "/usr/local/apache24/conf/httpd.conf"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  Require all granted
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap24_64.so
WrtOriginID HU:linux-tzsi_httpd:HUS
```

Ejemplo de archivo de correlaciones de alias de instancia

```
# Correlación de alias de instancia de Monitoring Agent for HTTP Server
# INSTANCE: descubierto automáticamente por agente. Por favor, NO modificar.
# ALIAS: nombre de alias para la instancia. El nombre se visualizará en el
# panel de instrumentos de IU de APM. Debe ser único
# entre todas las instancias y debe ser menor de 10 caracteres y constar sólo de caracteres
alfanuméricos.
#
INSTANCE.1=/usr/local/apache24/conf/httpd.conf
ALIAS.1=httpd

INSTANCE.1=/usr/local/apache24/conf/admin.conf
ALIAS.1=admin
```

Configuración de la supervisión de IBM Cloud

Monitoring Agent for IBM Cloud recopila inventario de máquina virtual y métricas de la cuenta IBM Cloud (SoftLayer). Utilice el agente de IBM Cloud para realizar el seguimiento de cuántos dispositivos virtuales se han configurado y se están ejecutando en IBM Cloud. Puede ver qué recursos se asignan a cada dispositivo virtual en la página del panel de instrumentos detallada, que también muestra información como el centro de datos en el que se encuentra un dispositivo, el sistema operativo y el ancho de banda de red público proyectado para el mes.

Antes de empezar

- Lea todo el tema “Configuración de la supervisión de IBM Cloud” en la página 282 para determinar qué se necesita para completar la configuración.
- Las instrucciones siguientes son para el release más reciente del agente, a excepción de lo indicado.
- Asegúrese de que los requisitos del sistema del Agente de IBM Cloud se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de IBM Cloud.
- Asegúrese de que la siguiente información está disponible:

– Un nombre de usuario para un usuario con al menos permisos de Auditor.
– La clave de API para IBM Cloud para ese usuario asociado.

Acerca de esta tarea

El Agente de IBM Cloud es un agente de varias instancias y también un agente de subnodo. Después de configurar instancias de agente, debe iniciar manualmente cada instancia de agente.

Procedimiento

1. Configure el agente en sistemas Windows mediante la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
   - "Configuración del agente en sistemas Windows" en la página 283.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 284.
2. Configure el agente en sistemas Linux con el script que solicita respuestas o el archivo de respuestas silencioso.
   - "Configuración del agente respondiendo a solicitudes" en la página 284.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 284.

Qué hacer a continuación

En la Consola de Cloud APM, vaya al Panel de instrumentos del rendimiento de aplicaciones para ver los datos que se han recopilado. Para obtener más información sobre la utilización de la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si no puede ver los datos en los paneles de instrumentos del agente, consulte primero los registros de conexión del servidor y, a continuación, los registros del proveedor de datos. Las vías de acceso a estos registros se listan aquí:

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Si desea recibir ayuda con la resolución de problemas, consulte el Foro de Cloud Application Performance Management.

Configuración del agente en sistemas Windows

Puede configurar el Agente de IBM Cloud en sistemas operativos Windows utilizando la ventana de IBM Cloud Application Performance Management. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la plantilla **Monitoring Agent for IBM Cloud** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar una instancia de agente por primera vez, la opción **Configurar el agente** no está disponible. Para configurar la instancia de agente de nuevo, púlsela con el botón derecho del ratón y luego pulse **Reconfigurar...**.
3. Especifique un nombre de instancia exclusivo y luego pulse **Aceptar**. Utilice solo letras latinas, números arábigos y el carácter de guión o signo menos en el nombre de instancia. Ejemplo, `icloud-inst`.
4. Pulse **Siguiente** en la ventana de nombre de instancia de agente.
5. Pulse **Nuevo** y escriba los valores de nombre de usuario de IBM Cloud SoftLayer y de clave de API y, a continuación, pulse **Siguiente**.

6. Pulse **Aceptar** para completar la configuración.
7. En la ventana de IBM Cloud Application Performance Management, pulse con el botón derecho del ratón la instancia que ha configurado y luego pulse **Iniciar**.

Configuración del agente respondiendo a solicitudes

Después de la instalación del Agente de IBM Cloud, debe configurarlo para poder iniciar el agente. Si el Agente de IBM Cloud está instalado en un sistema Linux local, puede seguir estas instrucciones para configurarlo de forma interactiva a través de las solicitudes de la línea de mandatos.

Acerca de esta tarea

Recuerde: Si está volviendo a configurar una instancia de agente configurada, se visualiza el valor que se establece en la última configuración para cada opción. Si desea borrar un valor existente, pulse la tecla de espacio cuando se visualice el valor.

Procedimiento

Siga estos pasos para configurar el Agente de IBM Cloud ejecutando un script y respondiendo a solicitudes.

1. Ejecute el mandato siguiente:

   ```
   dir_instalación/bin/ibm_cloud-agent.sh config nombre_instancia
   ```

   donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/ibm_cloud-agent.sh config icloud-inst
   ```

2. Responda a las solicitudes para establecer valores de configuración para el agente.

   Consulte la sección “Parámetros de configuración para el Agente de IBM Cloud” en la página 285 para obtener una descripción de cada uno de los parámetros de configuración.

3. Ejecute el mandato siguiente para iniciar el agente:

   ```
   dir_instalación/bin/ibm_cloud-agent.sh start nombre_instancia
   ```

   Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/ibm_cloud-agent.sh start icloud-inst
   ```

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

- Configure el Agente de IBM Cloud en modalidad silenciosa:
  a) Abra el archivo `ibm_cloud_silent_config.txt` de una de las vías de acceso siguientes en un editor de texto.
     – Linux *dir_instalación*`/samples/ibm_cloud_silent_config.txt`

       Ejemplo, `/opt/ibm/apm/agent/samples/ibm_cloud_silent_config.txt`
     – Windows *dir_instalación*`\samples\ibm_cloud_silent_config.txt`

       Ejemplo, `C:\IBM\APM\samples\ibm_cloud_silent_config.txt`

     Donde *dir_instalación* es la vía de acceso donde está instalado el agente.
  b) En el archivo `ibm_cloud_silent_config.txt`, especifique valores para todos los parámetros obligatorios y modifique los valores predeterminados de otros parámetros según sea necesario.

     Consulte "Parámetros de configuración para el Agente de IBM Cloud" en la página 285 para obtener una descripción de cada uno de los parámetros de configuración.
  c) Guarde y cierre el archivo `ibm_cloud_silent_config.txt` y ejecute el siguiente mandato:
     – Linux *dir_instalación*`/bin/ibm_cloud-agent.sh config` **nombre_instancia** *dir_instalación*`/samples/ibm_cloud_silent_config.txt`

       Ejemplo, **`/opt/ibm/apm/agent/bin/ibm_cloud-agent.sh config icloud-inst /opt/ibm/apm/agent/samples/ibm_cloud_silent_config.txt`**
     – Windows *dir_instalación*`\bin\ibm_cloud-agent.bat config` **nombre_instancia** *dir_instalación*`\samples\ibm_cloud_silent_config.txt`

       Ejemplo, **`C:\IBM\APM\bin\ibm_cloud-agent.bat config icloud-inst C:\IBM\APM\samples\ibm_cloud_silent_config.txt`**

     Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

     Importante: Asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.
  d) Ejecute el mandato siguiente para iniciar el agente:
     – Linux *dir_instalación*`/bin/ibm_cloud-agent.sh start` **nombre_instancia**

       Ejemplo, **`/opt/ibm/apm/agent/bin/ibm_cloud-agent.sh start icloud-inst`**
     – Windows *dir_instalación*`\bin\ibm_cloud-agent.bat start` **nombre_instancia**

       Ejemplo, **`C:\IBM\APM\bin\ibm_cloud-agent.bat start icloud-inst`**

     Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

Parámetros de configuración para el Agente de IBM Cloud

Los parámetros de configuración del Agente de IBM Cloud se visualizan en una tabla.

1. Configuración de IBM Cloud - Valores para supervisar las instancias de IBM Cloud de forma remota. Las instancias se descubren de forma automática para la clave de API que desea configurar.

Tabla 23. Configuración de IBM Cloud

Nombre de parámetro	Descripción	Nombre de parámetro del archivo de configuración silenciosa
Nombre de usuario	El nombre de usuario para la cuenta de IBM SoftLayer que se utiliza para recuperar las métricas de la API de IBM Cloud.	**KFS_USERNAME**

Tabla 23. Configuración de IBM Cloud (continuación)		
Nombre de parámetro	**Descripción**	**Nombre de parámetro del archivo de configuración silenciosa**
Clave de API	La clave de API específica de usuario necesaria para completar la autenticación. Las claves de API se generan y se pueden recuperar desde el portal de clientes de IBM SoftLayer.	**KFS_API_KEY_PASSWORD**

Configuración de la supervisión de IBM Integration Bus

El Agente de IBM Integration Bus es un agente de múltiple instancia. Debe crear una primera instancia de agente e iniciarla manualmente.

Antes de empezar

- Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.
- Asegúrese de que los requisitos del sistema del Agente de IBM Integration Bus se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Informe de requisitos del sistema detallados para el Agente de IBM Integration Bus.

Acerca de esta tarea

El procedimiento siguiente es una hoja de ruta para configurar el Agente de IBM Integration Bus, que incluye los pasos obligatorios y opcionales. Siga los pasos necesarios según sus necesidades.

Procedimiento

1. Asegúrese de que el ID de usuario que utilizará para iniciar y detener el Agente de IBM Integration Bus pertenece a los grupos de usuarios **mqm** y **mqbrkrs**.
2. Windows
   Si tiene instalado IBM MQ (WebSphere MQ) en el sistema Windows, añada la vía de acceso a la biblioteca de IBM MQ (WebSphere MQ) a la variable de entorno **PATH**. De ese modo, el Agente de IBM Integration Bus podrá cargar las bibliotecas de IBM MQ (WebSphere MQ) necesarias para el inicio.
   a) Añada la vía de acceso a biblioteca de IBM MQ (WebSphere MQ) al principio de la variable de entorno **PATH**.

      Por ejemplo, si la vía de acceso de instalación de IBM MQ (WebSphere MQ) es `C:\IBM\WMQ75`, añada `C:\IBM\WMQ75\bin` al principio de la variable de entorno **PATH** del sistema Windows.
   b) Reinicie el sistema Windows para que los cambios entren en vigor.
3. Configure el Agente de IBM Integration Bus especificando los siguientes parámetros de configuración. Hay también algunos parámetros de configuración opcionales que puede especificar para el agente. Para obtener instrucciones detalladas, consulte "Configuración del Agente de IBM Integration Bus" en la página 287.
   - ID de agente
   - El directorio de instalación de los nodos de integración (intermediarios) que se van a supervisar
   - La vía de acceso a biblioteca de 64 bits de IBM MQ (WebSphere MQ)
4. Configure IBM Integration Bus para habilitar los datos que desea supervisar. Consulte "Configuración de IBM Integration Bus para la habilitación de datos" en la página 291.

5. Si ha habilitado la recopilación de datos de instantánea para el nodo de integración (intermediario), configure el Agente de IBM Integration Bus para no almacenar los datos de instantánea. Para obtener instrucciones, consulte "Inhabilitación de la recopilación de datos de instantánea para el agente" en la página 298.
6. Opcional: Para configurar el Agente de IBM Integration Bus para habilitar el rastreo de transacciones, utilice la página **Configuración de agente**. Para obtener instrucciones, consulte "Configuración del rastreo de transacciones para el Agente de IBM Integration Bus" en la página 299.
7. Opcional: Si ya no necesita la función de rastreo de transacciones o desea desinstalar el Agente de IBM Integration Bus, inhabilite el rastreo de transacciones para IBM Integration Bus y elimine la salida de usuario proporcionada por el agente. Para obtener instrucciones, consulte las secciones "Inhabilitación del rastreo de transacciones" en la página 298 y "Eliminación de la salida de usuario KQIUserExit" en la página 301.

Configuración del Agente de IBM Integration Bus

Debe asignar un nombre de instancia al Agente de IBM Integration Bus y configurar el agente antes de poder empezar a supervisar el entorno de IBM Integration Bus.

Antes de empezar

- Asegúrese de que el ID de usuario que se utiliza para iniciar y detener el agente pertenece a los grupos de usuarios **mqm** y **mqbrkrs**.
- Windows Si tiene instalado IBM MQ (WebSphere MQ) en el sistema Windows, añada la vía de acceso a la biblioteca de IBM MQ (WebSphere MQ) a la variable de entorno **PATH**. De ese modo, el Agente de IBM Integration Bus podrá cargar las bibliotecas de IBM MQ (WebSphere MQ) necesarias para el inicio.
  1. Añada la vía de acceso a biblioteca de IBM MQ (WebSphere MQ) al principio de la variable de entorno **PATH**.

     Por ejemplo, si la vía de acceso de instalación de IBM MQ (WebSphere MQ) es `C:\IBM\WMQ75`, añada `C:\IBM\WMQ75\bin` al principio de la variable de entorno **PATH** del sistema Windows.
  2. Reinicie el sistema Windows para que los cambios entren en vigor.
- Puede que necesite proporcionar la información siguiente en función del entorno durante la configuración del agente. Si no conoce el valor de configuración adecuado que debe especificar, recopile la información del administrador de IBM MQ (WebSphere MQ) e IBM Integration Bus.
  - Si IBM MQ (WebSphere MQ) está instalado en el mismo sistema con el Agente de IBM Integration Bus, debe especificar la vía de acceso a biblioteca de 64 bits de IBM MQ (WebSphere MQ).
  - Si el Agente de IBM Integration Bus está configurado para supervisar los nodos de integración de IBM Integration Bus V10 o IBM App Connect Enterprise V11, debe proporcionar el directorio de instalación de IBM Integration Bus V10 o IBM App Connect Enterprise V11.
  - Si desea que el Agente de IBM Integration Bus supervise algunos nodos de integración (intermediarios) específicos en lugar de todos los del mismo sistema, debe especificar el nombre y la vía de instalación de cada nodo de integración (intermediario).

Acerca de esta tarea

El Agente de IBM Integration Bus es un agente de varias instancias; debe crear la primera instancia e iniciar el agente de forma manual.

Puede elegir configurar el agente con o sin interacciones en sistemas UNIX o Linux. En sistemas Windows, sólo puede configurar el agente sin interacciones.

- Para configurar el agente con interacción, ejecute el script de configuración y responda a las solicitudes. Consulte "Configuración interactiva" en la página 288.
- Para configurar el agente sin interacción, edite el archivo de respuestas silencioso y, a continuación, ejecute el script de configuración. Consulte "Configuración silenciosa" en la página 289.

Importante: si también ha instalado ITCAM Agent for WebSphere Message Broker, que se entrega como uno de los productos de ITCAM for Applications, en el mismo sistema que el Agente de IBM Integration Bus, que se entrega en Cloud APM, no los utilice para supervisar el mismo nodo de integración (intermediario) en el sistema.

Configuración interactiva

Procedimiento

Para configurar el agente mediante la ejecución del script y las respuestas a las solicitudes, siga estos pasos:

1. Especifique el mandato siguiente:

   ```
   dir_instalación/bin/iib-agent.sh config nombre_instancia
   ```

   donde *nombre_instancia* es el nombre que desea proporcionar a la instancia de agente.

   Importante: La configuración interactiva no está soportada en sistemas Windows.
2. Después de confirmar que desea configurar el Agente de IBM Integration Bus, especifique los valores de configuración para los valores generales del agente.
   a) Cuando se le solicite el parámetro **ID de agente**, especifique una serie alfanumérica exclusiva con una longitud máxima de 8 caracteres.

      Recuerde: la longitud máxima de ID de agente ha cambiado a 8 caracteres a partir de Agente de IBM Integration Bus versión 7.3.0.1. Para las versiones anteriores, la longitud máxima del ID de agente es de 4 caracteres.

      El nombre del sistema gestionado incluye el ID del agente que especifique, por ejemplo, *nombreintermediariosupervisado*:*idAgente*:KQIB, donde *nombreintermediariosupervisado* es el nombre del nodo de integración (intermediario) supervisado.
   b) Cuando se le solicite el parámetro de directorio de instalación de **IIB versión 10 o ACE versión 11**, si desea supervisar nodos de integración de IBM Integration Bus V10 o IBM App Connect Enterprise V11, especifique el directorio de instalación de IBM Integration Bus V10 o IBM App Connect Enterprise V11. Por ejemplo, `/opt/ibm/mqsi/ace-11.0.0.3`. Si no desea supervisar IBM Integration Bus V10 e IBM App Connect Enterprise V11, pulse Intro para aceptar el valor predeterminado.

      Recuerde: Puede especificar sólo un directorio de instalación para el parámetro de directorio de instalación de **IIB versión 10 o ACE versión 11**. Si ha instalado IBM Integration Bus V10 o IBM App Connect Enterprise V11 en diferentes directorios y desea supervisarlos todos, cree varias instancias de agente y especifique un directorio de instalación de IBM Integration Bus V10 o IBM App Connect Enterprise V11 para cada instancia de agente.
3. Opcional: Utilice la sección **Valores del intermediario supervisado** para especificar si desea utilizar este agente para supervisar solo algunos nodos de integración (intermediarios) específicos.

   De forma predeterminada, se supervisan todos los nodos de integración (intermediarios) que se ejecutan en el mismo sistema host que el Agente de IBM Integration Bus, tal como lo ha determinado el autodescubrimiento. Si desea que el agente supervise algunos nodos de integración (intermediarios) específicos, especifique el nombre del nodo de integración (intermediario) que desea supervisar y establezca el valor de **Recopilar datos de nodo** en No, que es el valor predeterminado, en la sección **Valores del intermediario supervisado**. Puede haber varias secciones **Valores del intermediario supervisado**. Cada sección controla los valores de supervisión para un nodo de integración (intermediario).

   Consejo: Puede especificar más de una sección **Valores del intermediario supervisado**. Al editar la sección **Valores del intermediario supervisado**, están disponibles las opciones siguientes:

   - Añadir: para crear una sección **Valores del intermediario supervisado** y configurarla para otro nodo de integración (intermediario).
   - Editar: para modificar los valores de la sección **Valores del intermediario supervisado** actual.

- Suprimir: para suprimir la sección **Valores del intermediario supervisado** actual.
- Siguiente: para trasladarse a la sección **Valores del intermediario supervisado** siguiente.
- Salir: para salir de la configuración de **Valores del intermediario supervisado**.

4. Si confirma que IBM MQ (WebSphere MQ) está instalado en el mismo sistema, se le solicitará el parámetro **Vía de acceso a biblioteca de WebSphere MQ de 64 bits**. Pulse Intro para aceptar el valor predeterminado, que es la vía de acceso a biblioteca de 64 bits de IBM MQ (WebSphere MQ) descubierta automáticamente por el agente. Si no se visualiza ningún valor predeterminado, debe proporcionar la vía de acceso a biblioteca de 64 bits de IBM MQ (WebSphere MQ) antes de continuar con el paso siguiente. Por ejemplo, `/opt/mqm8/lib64`.

   Recuerde: si los nodos de integración (intermediarios) utilizan distintas versiones de los gestores de colas, especifique la última versión de la vía de acceso de biblioteca de 64 bits de IBM MQ(WebSphere MQ) para este parámetro.
5. Una vez finalizada la configuración, especifique el mandato siguiente para iniciar el agente:

   ```
   dir_instalación/bin/iib-agent.sh start nombre_instancia
   ```

Configuración silenciosa

Procedimiento

Para configurar el agente mediante la edición del archivo de respuestas silenciosas y la ejecución del script sin interacción, siga estos pasos:

1. Abra el archivo de respuestas silencioso siguiente en un editor de texto.
   - Linux AIX *dir_instalación*`/samples/iib_silent_config.txt`
   - Windows *dir_instalación*`\tmaitm6_x64\samples\qi_silent_config.txt`

   Donde *dir_instalación* es el directorio de instalación del Agente de IBM Integration Bus. El directorio de instalación predeterminado es como sigue:
   - Linux AIX `/opt/ibm/apm/agent`
   - Windows `C:\IBM\APM`
2. Para el parámetro **agentId**, especifique una serie alfanumérica exclusiva con una longitud máxima de 8 caracteres como identificador corto para el agente.

   Recuerde: la longitud máxima de ID de agente ha cambiado a 8 caracteres a partir de Agente de IBM Integration Bus versión 7.3.0.1. Para las versiones anteriores, la longitud máxima del ID de agente es de 4 caracteres.

   El nombre del sistema gestionado incluye el ID del agente que especifique, por ejemplo, *nombreintermediariosupervisado*`:`*idAgente*`:KQIB`, donde *nombreintermediariosupervisado* es el nombre del nodo de integración (intermediario) supervisado.
3. Si desea supervisar los nodos de integración de IBM Integration Bus V10 o IBM App Connect Enterprise V11, especifique el directorio de instalación de IBM Integration Bus V10 o de IBM App Connect Enterprise V11 para el parámetro **defaultWMBInstallDirectory**. Por ejemplo, `C:\Archivos de programa\IBM\ACE\11.0.0.3\` para un sistema Windows, o `/opt/ibm/mqsi/ace-11.0.0.3` para un sistema Linux. Si no desea supervisar IBM Integration Bus V10 e IBM App Connect Enterprise V11, este parámetro no es necesario, ya que el Agente de IBM Integration Bus puede descubrir automáticamente los nodos de integración (intermediarios) de las versiones anteriores.

   Recuerde: puede especificar solo un directorio de instalación para el parámetro **defaultWMBInstallDirectory**. Si ha instalado IBM Integration Bus V10 o IBM App Connect Enterprise V11 en diferentes directorios y desea supervisarlos todos, cree varias instancias de agente y especifique un directorio de instalación de IBM Integration Bus V10 o IBM App Connect Enterprise V11 para cada instancia de agente.

4. Opcional: Especifique si desea utilizar este agente para supervisar solo algunos nodos de integración (intermediarios) específicos.

   De forma predeterminada, se supervisan todos los nodos de integración (intermediarios) que se ejecutan en el mismo sistema host que el Agente de IBM Integration Bus, tal como lo ha determinado el autodescubrimiento. Para supervisar nodos de integración (intermediarios) específicos, establezca los parámetros **collectNodeData** y **WMBInstallDirectory** para cada nodo de integración (intermediario) que desee supervisar.

   collectNodeData
   Especifica si los datos de definición de nodo se recopilan para el nodo de integración (intermediario) supervisado. La sintaxis es `collectNodeData.`*`nombre_intermediario`*`=NO|YES`, donde *nombre_intermediario* es el nombre del nodo de integración (intermediario).

   El valor predeterminado es NO. Se recomienda utilizar el valor predeterminado, porque los datos de definición de nodo no están soportados en la Consola de Cloud APM.

   WMBInstallDirectory
   El directorio de instalación del nodo de integración (intermediario) que se va a supervisar. La sintaxis es `WMBInstallDirectory.`*`nombre_intermediario=dir_instalación_intermediario`*, donde *dir_instalación_intermediario* es el directorio de instalación del nodo de integración (intermediario) que se va a supervisar.

   Recuerde: En el caso de un nodo de integración de la versión 10, el parámetro **WMBInstallDirectory** puede alterar temporalmente el parámetro **defaultWMBInstallDirectory** que ha establecido en el paso anterior.

   Por ejemplo, para supervisar sólo dos nodos de integración (intermediarios) denominados BK1 y BK2, establezca los parámetros tal como se indica a continuación:

   ```
   collectNodeData.BK1=NO
   collectNodeData.BK2=NO
   WMBInstallDirectory.BK1=dir_instal_BK1
   WMBInstallDirectory.BK2=dir_instal_BK2
   ```

5. Para supervisar intermediarios anteriores a IBM Integration Bus V10, especifique la vía de acceso a biblioteca de 64 bits de IBM MQ(WebSphere MQ) para el parámetro **WMQLIBPATH**. Por ejemplo, `C:\Archivos de programa\IBM\WebSphere MQ\bin64` para un sistema Windows, o `/opt/mqm8/lib64` para un sistema Linux.

   Recuerde: si los nodos de integración (intermediarios) utilizan distintas versiones de los gestores de colas, especifique la última versión de la vía de acceso de biblioteca de 64 bits de IBM MQ(WebSphere MQ) para este parámetro.

6. Guarde y cierre el archivo de respuestas silencioso del agente y luego especifique el mandato siguiente:

   - Linux AIX *dir_instalación*`/bin/iib-agent.sh config `*nombre_instancia vía_acceso_a_archivo_respuestas*
   - Windows *dir_instalación*`\BIN\iib-agent.bat config "`*nombre_instancia vía_acceso_a_archivo_respuestas*`"`

   Donde *nombre_instancia* es el nombre de la instancia que configura, y *vía_acceso_archivo_respuestas* es la vía de acceso completa del archivo de respuestas silencioso.

   Aviso: En sistemas Windows, no incluya comillas dobles ("") que rodean la vía de acceso completa al archivo de respuestas silencioso, ya que esto causará un error de configuración.

7. Una vez finalizada la configuración, especifique el mandato siguiente para iniciar el agente:

   - Linux AIX

     ```
     dir_instalación/bin/iib-agent.sh start nombre_instancia
     ```

- Windows

```
dir_instalación\bin\iib-agent.bat start nombre_instancia
```

Resultados

Ahora, puede iniciar la sesión en la Consola de Cloud APM y utilizar el editor de aplicaciones para añadir la instancia del Agente de IBM Integration Bus al Panel de instrumentos del rendimiento de aplicaciones. Si desea instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte "Gestión de aplicaciones" en la página 1133.

Recuerde: cada vez que actualice o migre un nodo de integración supervisado, debe reiniciar el Agente de IBM Integration Bus después de la actualización o migración del nodo de integración (intermediario).

Qué hacer a continuación

El siguiente paso consiste en configurar IBM Integration Bus para la habilitación de datos. Los datos siguientes sólo están disponibles en el Panel de instrumentos del rendimiento de aplicaciones después de habilitarlos en IBM Integration Bus:

- Estadísticas y contabilidad de archivado
- Estadísticas de recursos de JVM
- Rastreo de transacciones

Encontrará instrucciones en: "Configuración de IBM Integration Bus para la habilitación de datos" en la página 291.

Configuración de IBM Integration Bus para la habilitación de datos

Para que algunos datos estén disponibles en la Consola de Cloud APM, debe configurar IBM Integration Bus para habilitar la recopilación de datos necesaria.

Antes de empezar

Asegúrese de que el Agente de IBM Integration Bus esté configurado.

Recuerde: la habilitación del rastreo de transacciones exige el reinicio del nodo de integración (intermediario).

Acerca de esta tarea

El Agente de IBM Integration Bus sólo puede supervisar estadísticas de archivado y de recursos después de habilitar la recopilación de datos para el nodo de integración (intermediario). Del mismo modo, si desea visualizar el rastreo de transacciones en los paneles de instrumentos de middleware y topología, debe habilitar el rastreo de transacciones dentro del nodo de integración (intermediario) antes de habilitar el rastreo de transacciones para el Agente de IBM Integration Bus..

Decida qué tipo de datos debe supervisar con el Agente de IBM Integration Bus y siga estos pasos según sus necesidades.

Los servidores de integración que son propiedad del nodo de integración tienen un archivo de configuración `server.conf.yaml` predeterminado para cada servidor de integración que se almacena en un subdirectorio del directorio de nodo de integración. Las propiedades que establezca para el nodo de integración en el archivo `node.conf.yaml` son heredadas por los servidores de integración de los que es propietario. Sin embargo, puede cambiar las propiedades de un servidor de integración modificándolas en su archivo `server.conf.yaml`. (Para obtener más información, consulte Configuración de un nodo de integración modificando el archivo node.conf.yaml en la documentación de IBM App Connect Enterprise).

Procedimiento

- Para habilitar la recopilación de datos de estadísticas de archivado para el nodo de integración (intermediario), consulte "Habilitación de la recopilación de datos de estadísticas y contabilidad de archivado" en la página 292.
- Para habilitar la recopilación de datos de estadísticas de recursos para un nodo de integración (intermediario), consulte "Estadísticas de estadísticas de recursos de JVM" en la página 295.
- Para habilitar el rastreo de transacciones para los flujos de mensajes dentro del nodo de integración (intermediario), consulte "Habilitación del rastreo de transacciones" en la página 296.
- Si ya no desea datos de rastreo de transacciones, recuerde que debe inhabilitar el rastreo de transacciones para el nodo de integración (intermediario) en el que se ha habilitado. Consulte "Inhabilitación del rastreo de transacciones" en la página 298.

Habilitación de la recopilación de datos de estadísticas y contabilidad de archivado

Acerca de esta tarea

Para habilitar la recopilación de estadísticas y contabilidad de archivados para flujos de mensajes que pertenecen al nodo de integración (intermediario), emita el mandato **mqsichangeflowstats** desde el directorio `bin` del directorio de instalación del nodo de integración (intermediario) .

Recuerde: emita el mandato **mqsichangeflowstats** para el nodo de integración (intermediario) de acuerdo con sus requisitos para la supervisión de datos. Se recomienda que habilite solo las estadísticas que necesita, porque puede haber una gran cantidad de datos y proceso cuando se tienen muchos flujos de mensajes. Si desea información más detallada sobre el mandato **mqsichangeflowstats**, consulte la documentación de IBM Integration Bus.

Importante: IBM Cloud Application Performance Management no soporta los datos estadísticos y de contabilidad de instantáneas debido a la cantidad de datos y el proceso necesarios para el intervalo de instantánea establecido en 20 segundos. Los datos de archivado proporcionan los mismos atributos exactos que datos de instantánea, y son más aptos para la supervisión de producción regular proporcionada por IBM Cloud Application Performance Management. Si ha habilitado la recopilación de datos de instantánea para el nodo de integración (intermediario), recuerde configurar Agente de IBM Integration Bus para no almacenar los datos de instantánea. Si desea más instrucciones, consulte "Inhabilitación de la recopilación de datos de instantánea para el agente" en la página 298.

Procedimiento

- Para obtener la mayoría de datos de los flujos de mensajes, emita el mandato siguiente. Este mandato es aconsejable porque no habilita las estadísticas de terminal más detalladas que proporcionan recuentos de invocaciones por terminal y por nodo. El nivel de terminal consume una gran cantidad de almacenamiento.

```
mqsichangeflowstats
nombre_intermediario
-a
-g -j -c active -t none -n basic -o xml
```

- En ACE versión 11, para obtener la mayoría de los datos para flujos de mensajes, modifique el archivo `node.conf.yaml` o `server.conf.yaml` como se indica a continuación. Estas propiedades se recomiendan porque no habilitan las estadísticas de terminal más detalladas que proporcionan recuentos de invocación por terminal y por nodo. El nivel de terminal consume una gran cantidad de almacenamiento.

```
Estadísticas:
  # Los flujos de mensajes de aplicación heredarán de forma predeterminada los valores de
Instantánea y Archivador
  # establecidos aquí
  Instantánea:
    #publicationOn: 'inactive' # elija 1 de : active|inactive, valor predeterminado inactive
                               # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                               # se ha establecido para outputFormat json,xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
```

```
    #nodeDataLevel: 'none'     # elija 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por comas de:
                               #csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # elija 1 de : none|basic
  Archivador:
    archivalOn: 'active'     # elija 1 de : active|inactive,
                             # valor predeterminado inactive
                               # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                               # se ha establecido para formato de salida xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    #majorInterval: 60         # Establece el intervalo en minutos con el que
                               # se publican las estadísticas de archivado
    nodeDataLevel: 'basic'         # elija 1 de : none|basic|advanced
    outputFormat: 'xml' # lista separada por comas de : csv,xml,usertrace
    #threadDataLevel: 'none'   # elija 1 de : none|basic
```

Nota: Si desea inhabilitar este valor, comente las líneas de **archivalOn: 'active'**, **nodeDataLevel: 'basic'** y **outputFormat: 'xml'**.

- Para obtener todos los datos soportados por el Agente de IBM Integration Bus, emita el mandato siguiente:

```
mqsichangeflowstats
nombre_intermediario -a -g -j -c active -t
none -n
advanced -o xml
```

- En ACE versión 11, para obtener todos los datos soportados por el Agente de IBM Integration Bus, modifique el archivo `node.conf.yaml` o `server.conf.yaml` como se indica a continuación:

```
Estadísticas:
  # Los flujos de mensajes de aplicación heredarán de forma predeterminada los valores de
Instantánea y Archivador
  # establecidos aquí
  Instantánea:
    #publicationOn: 'inactive' # elija 1 de : active|inactive, valor predeterminado inactive
                               # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                               # se ha establecido para outputFormat json,xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    #nodeDataLevel: 'none'     # elija 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por comas de:
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # elija 1 de : none|basic
  Archivador:
    archivalOn: 'active'    # elija 1 de : active|inactive, valor predeterminado inactive
                               # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                               # se ha establecido para formato de salida xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    #majorInterval: 60         # Establece el intervalo en minutos con el que
                               # se publican las estadísticas de archivado
    nodeDataLevel: 'advanced'         # elija 1 de : none|basic|advanced
    outputFormat: 'xml' # lista separada por comas de : csv,xml,usertrace
    #threadDataLevel: 'none'   # elija 1 de : none|basic
```

Nota: Si desea inhabilitar este valor, comente las líneas de **archivalOn: 'active'**, **nodeDataLevel: 'advanced'** y **outputFormat: 'xml'**.

- Para reducir la cantidad de datos pero seguir supervisando de forma razonable todos los flujos de mensajes sin más detalles, emita el mandato siguiente:

```
mqsichangeflowstats
nombre_intermediario
-a -g
-j -c active -t none -n none -o xml
```

- En ACE versión 11, para reducir la cantidad de datos pero seguir supervisando de forma razonable todos los flujos de mensajes sin más detalles, modifique el archivo `node.conf.yaml` o `server.conf.yaml` del siguiente modo:

```
Estadísticas:
  # Los flujos de mensajes de aplicación heredarán de forma predeterminada los valores de
Instantánea y Archivador
  #establecidos aquí
  Instantánea:
    #publicationOn: 'inactive' # elija 1 de : active|inactive, valor predeterminado inactive
```

```
                              # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                              # se ha establecido para outputFormat json,xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    #nodeDataLevel: 'none'     # elija 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por comas de:
                              # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # elija 1 de : none|basic
  Archivador:
    archivalOn: 'active'    # elija 1 de : active|inactive, valor predeterminado inactive
                              # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                              # se ha establecido para formato de salida xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    #majorInterval: 60         # Establece el intervalo en minutos con el que
                              # se publican las estadísticas de archivado
    nodeDataLevel: 'none'        # elija 1 de : none|basic|advanced
    outputFormat: 'xml' # lista separada por comas de : csv,xml,usertrace
    #threadDataLevel: 'none'   # elija 1 de : none|basic
```

Nota: Si desea inhabilitar este valor, comente las líneas de **archivalOn: 'active'**, **nodeDataLevel: 'none'** y **outputFormat: 'xml'**.

- Si tiene una gran cantidad de flujos de mensajes y desea reducir la cantidad de datos, puede especificar qué flujos de mensajes supervisar sustituyendo la opción `-g` o `-j` en los mandatos indicados.
  - Para especificar un servidor de integración concreto (grupo de ejecución) para la habilitación, sustituya `-g` con `-e` *`nombre_servidor_integración`*.
  - Para identificar un flujo de mensajes concreto para la habilitación, sustituya `-j` con `-f` *`nombre_flujo_mensajes`*.
  - Si ha agrupado los flujos de mensajes en aplicaciones, para especificar una aplicación concreta para la habilitación, añada `-k` *`nombre_aplicación`* a la opción `-j`.
- El Agente de IBM Integration Bus recopila datos de estadísticas y de contabilidad de archivado a intervalos de 5 minutos. Para establecer el intervalo con el que el nodo de integración (intermediario) genera los datos de estadísticas y contabilidad de archivado en el mismo intervalo, emita el mandato siguiente con el nodo de integración (intermediario) detenido y, después, reinícielo:

```
mqsichangebroker
nombre_intermediario -v
5
```

- En ACE versión 11, el Agente de IBM Integration Bus recopila datos de estadísticas y contabilidad de archivado a intervalos de 5 minutos. Para establecer el intervalo con el que el nodo de integración (intermediario) genera los datos de estadísticas y contabilidad de archivado en el mismo intervalo, modifique el archivo `node.conf.yaml` o `server.conf.yaml` del siguiente modo:

```
Estadísticas:
  # Los flujos de mensajes de aplicación heredarán de forma predeterminada los valores de
Instantánea y Archivador
  # establecidos aquí
  Instantánea:
    #publicationOn: 'inactive' # elija 1 de : active|inactive, valor predeterminado inactive
                              # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                              # se ha establecido para outputFormat json,xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    #nodeDataLevel: 'none'     # elija 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por comas de:
                              # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # elija 1 de : none|basic
  Archivador:
    archivalOn: 'active'       # elija 1 de : active|inactive, valor predeterminado inactive
                              # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                              # se ha establecido para formato de salida xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    majorInterval: 5         # Establece el intervalo en minutos a los
                              # se publican las estadísticas de archivado
    nodeDataLevel: 'none'      # elija 1 de : none|basic|advanced
    outputFormat: 'xml' # lista separada por comas de : csv,xml,usertrace
    #threadDataLevel: 'none'   # elija 1 de : none|basic
```

Resultados
Una vez configurado e iniciado el Agente de IBM Integration Bus, la contabilidad de flujo de mensajes y los estadísticos se visualizan en los siguientes widgets de grupo:

- Panel de instrumentos de flujo de mensaje
  - Confirmaciones y restituciones
  - Microsegundos de CPU
  - Microsegundos transcurridos
  - Velocidad de bytes de entrada
  - Velocidad de mensajes de entrada
  - Tamaño de mensaje de entrada
  - Microsegundos de CPU de espera de mensajes de entrada
  - Microsegundos transcurridos de espera de mensajes de entrada
  - Errores de flujo de mensajes
  - Estadísticas de nodos de proceso de mensajes
- Panel de instrumentos del nodo de proceso
  - Microsegundos de CPU
  - Microsegundos transcurridos
  - Invocaciones
  - Estado de nodo de proceso
  - Estadísticas de terminal

Estadísticas de estadísticas de recursos de JVM

Acerca de esta tarea
Para habilitar las estadísticas de recursos de JVM para los servidores de integración que pertenecen al nodo de integración (intermediario), emita el mandato **mqsichangeresourcestats** desde el directorio `bin` del directorio de instalación del nodo de integración (intermediario) .

Recuerde: las estadísticas de recursos de JVM se consideran opcionales porque solo se muestran unos pocos atributos de datos para el coste alto del agente que procesa estos datos cada 20 segundos. Asegúrese de que tiene en cuenta si realmente necesita los datos estadísticos de recurso de la JVM.

Procedimiento

- Para habilitar las estadísticas en todos los servidores de integración del nodo de integración (intermediario), emita el mandato siguiente:

```
mqsichangeresourcestats
nombre_intermediario -c active
```

- En ACE versión 11, para habilitar las estadísticas en todos los servidores de integración del nodo de integración (intermediario), modifique el archivo `node.conf.yaml` como se indica a continuación:

```
Estadísticas:
  # Los flujos de mensajes de aplicación heredarán de forma predeterminada los valores de
Instantánea y Archivador
  # establecidos aquí
  Instantánea:
    #publicationOn: 'inactive' # elija 1 de : active|inactive, valor predeterminado inactive
                               # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                               # se ha establecido para outputFormat json,xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    #nodeDataLevel: 'none'     # elija 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por comas de:
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # elija 1 de : none|basic
  Archivador:
```

```
    archivalOn: 'active'       # elija 1 de : active|inactive, valor predeterminado inactive
                               # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                               # se ha establecido para formato de salida xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    majorInterval: 5          # Establece el intervalo en minutos con el que
                              # se publican las estadísticas de archivado
    nodeDataLevel: 'advanced'     # elija 1 de : none|basic|advanced
    outputFormat: 'xml' # lista separada por comas de : csv,xml,usertrace
    threadDataLevel: 'basic'      # elija 1 de : none|basic
   Recurso:
     reportingOn: true       # elija 1 de : true|false, valor predeterminado false
......
```

Nota: Si desea inhabilitar este valor, comente **reportingOn: true**.

- Para habilitar las estadísticas para un servidor de integración determinado en el nodo de integración (intermediario), emita el mandato siguiente>

```
mqsichangeresourcestats
nombre_intermediario -e
nombre_servidor_integración -c
active
```

- En ACE versión 11, para habilitar las estadísticas de un servidor de integración determinado en el nodo de integración (intermediario), modifique el archivo `server.conf.yaml` como se indica a continuación:

```
Estadísticas:
  # Los flujos de mensajes de aplicación heredarán de forma predeterminada los valores de
Instantánea y Archivador
  # establecidos aquí
  Instantánea:
    #publicationOn: 'inactive' # elija 1 de : active|inactive, valor predeterminado inactive
                               # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                               # se ha establecido para outputFormat json,xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    #nodeDataLevel: 'none'     # elija 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por comas de:
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # elija 1 de : none|basic
  Archivador:
    archivalOn: 'active'       # elija 1 de : active|inactive, valor predeterminado inactive
                               # Asegúrese de que Events.OperationalEvents.MQ|MQTT
                               # se ha establecido para formato de salida xml
    #accountingOrigin: 'none'  # elija 1 de : none|basic
    majorInterval: 5           # Establece el intervalo en minutos con el que
                               # se publican las estadísticas de archivado
    nodeDataLevel: 'advanced'  # elija 1 de : none|basic|advanced
    outputFormat: 'xml' # lista separada por comas de : csv,xml,usertrace
    threadDataLevel: 'basic'      # elija 1 de : none|basic
  Recurso:
    reportingOn: true       # elija 1 de : true|false, valor predeterminado false
```

Nota: Si desea inhabilitar este valor, comente **reportingOn: true**.

Resultados

Los datos estadísticos de recursos JVM se visualizan en los siguientes widgets de grupo:

- Recuento de recogidas de basura
- Duración de recogida de basura
- Memoria no de almacenamiento dinámico de JVM
- Memoria de almacenamiento dinámico de JVM

Habilitación del rastreo de transacciones

Antes de empezar

1. Asegúrese de que se haya instalado el Agente de IBM Integration Bus. Se incluye una salida de usuario llamada `KQIUserExit` para habilitar IBM Integration Bus para el rastreo de transacciones.

2. Asegúrese de que el usuario que iniciará el nodo de integración (intermediario) tiene acceso al directorio de módulo de la salida de usuario de KQI. Es decir, asegúrese de añadir el ID de usuario que ha utilizado para iniciar el nodo de integración (intermediario) al grupo en el que ha instalado Agente de IBM Integration Bus.

Acerca de esta tarea

Debe desplegar la salida de usuario `KQIUserExit` en el nodo de integración (intermediario). De lo contrario, no habrá ningún dato disponible en el middleware ni en los paneles de instrumentos de topología incluso después de haber habilitado Agente de IBM Integration Bus para el rastreo de transacciones.

Consejo: La salida de usuario `KQIUserExit` incluye los nodos de IBM Integration Bus siguientes en los paneles de instrumentos de middleware y de topología como servicios no instrumentados:

- Nodos de cálculo y de base de datos donde se especifica un origen de datos ODBC
- Nodos TCP/IP
- Nodos de archivo para servidores FTP o FTPS remotos
- Nodos MQ, a no ser que ya estén instrumentados

Procedimiento

Para habilitar el rastreo de transacciones para IBM Integration Bus, complete los pasos siguientes:

1. Linux AIX
   Cierre los shell de intermediario que hayan cargado el entorno de MQSI.
2. Abra una consola de mandatos de IBM Integration Bus con uno de los métodos siguientes. Si tiene instaladas varias versiones de nodos de integración (intermediarios), asegúrese de iniciar la consola de mandatos para la versión correcta.
   - Windows Pulse **Inicio** > **IBM Integration Bus** > **IBM Integration Console**
   - Linux AIX En el directorio `bin` del directorio de instalación del nodo de integración (intermediario), emita el mandato **mqsiprofile**.
3. Detenga el nodo de integración (intermediario) que desea configurar con el mandato **mqsistop**.
4. Habilite el rastreo de transacciones para el flujo de mensajes dentro del nodo de integración (intermediario) añadiendo la salida de usuario KQIUserExit con el mandato **mqsichangebroker**.
   - Para habilitar el rastreo de transacciones para todos los flujos de mensajes dentro del nodo de integración (intermediario), ejecute el mandato siguiente:

     ```
     mqsichangebroker nombre_intermediario -e "KQIUserExit"
     ```

   - Para habilitar el rastreo de transacciones para un flujo de mensajes específico dentro del nodo de integración (intermediario), ejecute el mandato siguiente:

     ```
     mqsichangeflowuserexits
     nombre_intermediario -e nombre_grupo_ejecución -k nombre_aplicación -f
     nombre_flujo_mensajes -a "KQIUserExit"
     ```

5. Como alternativa, en Ace versión 11, habilite el rastreo de transacciones para el flujo de mensajes dentro del nodo de integración (intermediario) añadiendo `KQIUserExit` al archivo `node.conf.yaml` o `server.conf.yaml`.

   ```
   UserExits:
   activeUserExitList: 'KQIUserExit' # Especifique el nombre
   # de una salida de usuario instalada para activarla.
   ```

   Nota: Si desea inhabilitar el rastreo de transacciones, comente **activeUserExitList: 'KQIUserExit'**.
6. Reinicie el nodo de integración (intermediario) con el mandato **mqsistart**.

Inhabilitación del rastreo de transacciones

Procedimiento

Para inhabilitar el rastreo de transacciones para IBM Integration Bus, complete los pasos siguientes:

1. Abra una consola de mandatos de IBM Integration Bus con uno de los métodos siguientes. Si tiene instaladas varias versiones de nodos de integración (intermediarios), asegúrese de iniciar la consola de mandatos para la versión correcta.
   - Windows Pulse **Inicio** > **IBM Integration Bus** > **IBM Integration Console**
   - Linux AIX En el directorio `bin` del directorio de instalación del nodo de integración (intermediario), emita el mandato **mqsiprofile**.
2. Inhabilite el rastreo de transacciones para el flujo de mensajes dentro de un nodo de integración (intermediario) con uno de los métodos siguientes:
   - Para inhabilitar el rastreo de transacciones para un flujo de mensajes específico, utilice el mandato **mqsichangeflowuserexits**:

     ```
     mqsichangeflowuserexits nombre_intermediario -e nombre_grupo_ejecución
     -f nombre_flujo_mensajes -a ""
     ```

   - Para inhabilitar el rastreo de transacciones para todos los flujos de mensajes dentro del nodo de integración (intermediario), primero detenga el nodo de integración (intermediario) con el mandato **mqsistop** y luego emita el mandato **mqsichangebroker**:

     ```
     mqsichangebroker nombre_intermediario -e ""
     ```

Qué hacer a continuación

- Para el rastreo de transacciones, tras habilitar el rastreo de transacciones para IBM Integration Bus, también debe habilitar el rastreo de transacciones para el agente. Si desea más instrucciones, consulte “Configuración del rastreo de transacciones para el Agente de IBM Integration Bus” en la página 299.
- Si ha habilitado la recopilación de datos de instantánea para el nodo de integración (intermediario), configure el Agente de IBM Integration Bus para no almacenar los datos de instantánea. Cloud APM no soporta los datos estadísticos y de contabilidad de instantáneas debido a la cantidad de datos y el proceso necesarios para el intervalo de instantánea establecido en 20 segundos. Para obtener instrucciones, consulte “Inhabilitación de la recopilación de datos de instantánea para el agente” en la página 298.

Inhabilitación de la recopilación de datos de instantánea para el agente

Cloud APM no soporta los datos estadísticos y de contabilidad de instantáneas debido a la cantidad de datos y el proceso necesarios para el intervalo de instantánea establecido en 20 segundos. Si ha habilitado la recopilación de datos de instantánea para el intermediario, recuerde configurar Agente de IBM Integration Bus para no almacenar los datos de instantánea.

Procedimiento

1. Abra el archivo de configuración del agente en un editor de texto. El archivo de configuración del agente está en uno de los siguientes directorios en función del sistema operativo:
   - Linux AIX *dir_instalación*/config/<*nombre_host*>_qi_<*nombre_instancia*>.cfg
   - Windows *dir_instalación*\TMAITM6_x64\<*nombre_host*>_qi_<*nombre_instancia*>.cfg

   donde *dir_instalación* es el directorio de instalación de agente; *nombre_host* es el nombre de host del sistema operativo; *nombre_instancia* es el nombre de instancia de agente.
2. Edite el archivo añadiendo el siguiente parámetro en la sección KqiAgent:

```
defaultRetainRecentSnapshotSamples=0
```

Ejemplo:

```
INSTANCE=inst1 [
SECTION=KqiAgent [ { agentId=inst1 } { instName=inst1 }
{defaultRetainRecentSnapshotSamples=0}]
SECTION=MonitorBroker:BRK1 [ { collectNodeData=NO } ]
SECTION=MonitorBroker:BRK2 [ { collectNodeData=NO } ]
]
```

3. Guarde los cambios y cierre el archivo.
4. Reinicie Agente de IBM Integration Bus para que los cambios entren en vigor.

Configuración del rastreo de transacciones para el Agente de IBM Integration Bus

Los datos de rastreo de transacciones de IBM Integration Bus se pueden visualizar en los paneles de instrumentos de middleware y topología tras habilitar la recopilación de datos en la página **Configuración de agente** del Agente de IBM Integration Bus.

Antes de empezar

- Asegúrese de que el rastreo de transacciones éste habilitado para IBM Integration Bus con la salida de usuario proporcionada por el agente denominada `KQIUserExit`. Si aún no lo ha hecho, siga las instrucciones de la sección “Habilitación del rastreo de transacciones” en la página 296.
- Asegúrese de que el Agente de IBM Integration Bus esté configurado adecuadamente. Si aún no lo ha hecho, siga las instrucciones de la sección “Configuración del Agente de IBM Integration Bus” en la página 287.

Procedimiento

Para configurar el rastreo de transacciones para el Agente de IBM Integration Bus, realice estos pasos:

1. En la barra de navegación, pulse **Configuración del sistema** > **Configuración del agente**.
   Se mostrará la página **Configuración del agente**.
2. Pulse la pestaña **IBM Integration Bus**.
3. Seleccione los recuadros de selección de las instancias de agente y lleve a cabo una de las acciones siguientes de la lista **Acciones**:
   - Para habilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Habilitado**. El estado de la columna **Rastreo de transacciones** se actualizará a Habilitado.
   - Para inhabilitar los datos de rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Inhabilitado**. El estado de la columna **Rastreo de transacciones** se actualizará a Inhabilitado.

Resultados

Habrá configurado el rastreo de transacciones para las instancias de agente seleccionadas. Los datos de rastreo de transacciones se pueden visualizar en los paneles de instrumentos de middleware y topología, tras habilitar la recopilación de datos. Para obtener más información, consulte “Adición de aplicaciones middleware al Application Performance Dashboard” en la página 102.

Especificación de un nombre de sistema gestionado exclusivo para el Agente de IBM Integration Bus

El nombre de instancia de Agente de IBM Integration Bus que se visualiza en la Consola de Cloud APM se conoce también como nombre de sistema gestionado (MSN). Puede utilizar el parámetro de configuración del agente para especificar un MSN exclusivo para cada instancia de agente.

Acerca de esta tarea

Cuando se inicia el Agente de IBM Integration Bus, registra el MSN en el formato *nombre_intermediario_supervisado*:*IDagente*:KQIB para cada instancia de agente, donde

nombre_intermediario_supervisado es el nombre del intermediario supervisado e *IDagente* es el ID de agente establecido por el parámetro de configuración del agente. La longitud máxima del MSN es de 32 caracteres. Si la longitud del MSN supera los 32 caracteres, se trunca.

Puede ser necesario un MSN exclusivo en las circunstancias siguientes:

- Está ejecutando más de un Agente de IBM Integration Bus en el mismo sistema.
- Está ejecutando más de un intermediario supervisado con el mismo nombre en distintos sistemas.

Para especificar un ID de agente para obtener un MSN exclusivo, utilice la opción **ID de agente** durante la configuración interactiva o utilice el parámetro **agentId** en el archivo de respuestas silencioso.

Recuerde: si no ha configurado el Agente de IBM Integration Bus por primera vez después de la instalación, siga los pasos indicados en "Configuración del Agente de IBM Integration Bus" en la página 287.

Procedimiento

- Para utilizar la opción **ID de agente** durante la configuración interactiva, siga estos pasos:
  a) Especifique el mandato siguiente:

  ```
  dir_instalación/bin/iib-agent.sh config nombre_instancia
  ```

  donde *nombre_instancia* es el nombre de la instancia de agente para la que desea especificar un ID de agente.
  b) Siga las opciones para configurar la instancia de agente.
  Si no se necesita ningún cambio para una opción, utilice el valor predeterminado.
  c) Cuando aparezca la opción `ID de agente`, especifique el calificador medio para el nombre del sistema gestionado.
  El formato válido es una serie alfanumérica con una longitud máxima de 8 caracteres.
- Para utilizar el parámetro **agentId** en el archivo de respuestas silencioso, realice los siguientes pasos:
  a) Abra el archivo de respuestas silencioso siguiente en un editor de texto.
  – Linux AIX *dir_instalación*/samples/iib_silent_config.txt
  – Windows *dir_instalación*\tmaitm6_x64\samples\qi_silent_config.txt
  b) Especifique un ID de agente para el parámetro **agentId**.
  El formato válido es una serie alfanumérica con una longitud máxima de 8 caracteres.
  c) Guarde y cierre el archivo de respuestas silencioso y ejecute el mandato siguiente desde la línea de mandatos:
  – Linux AIX *dir_instalación*/bin/iib-agent.sh config *nombre_instancia vía_acceso_a_archivo_respuestas*
  – Windows *dir_instalación*\BIN\iib-agent.bat config "*nombre_instancia vía_acceso_a_archivo_respuestas*"
  Donde *nombre_instancia* es el nombre de la instancia que configura, y *vía_acceso_archivo_respuestas* es la vía de acceso completa del archivo de respuestas silencioso.

  Aviso: En sistemas Windows, no incluya comillas dobles ("") que rodean la vía de acceso completa al archivo de respuestas silencioso, ya que esto causará un error de configuración.
  d) Una vez finalizada la configuración, especifique el mandato siguiente para iniciar el agente:
  – Linux AIX

  ```
  dir_instalación/bin/iib-agent.sh start nombre_instancia
  ```

– Windows

```
dir_instalación\bin\iib-agent.bat start nombre_instancia
```

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM. Si la instancia de agente con el MSN anterior se sigue visualizando como fuera de línea, edite la aplicación para eliminarlo y luego añada la nueva instancia de agente con el ID de agente asignado.

Eliminación de la salida de usuario KQIUserExit

Antes de desinstalar el Agente de IBM Integration Bus, debe eliminar la salida de usuario `KQIUserExit`.

Procedimiento

Realice los pasos siguientes para eliminar la salida de usuario `KQIUserExit` que ha desplegado en IBM Integration Bus para el rastreo de transacciones:

1. Vaya al directorio `bin` del Agente de IBM Integration Bus.
   - Windows *dir_instalación_agente*`\`*arqu*`\qi\bin`
   - Linux AIX *dir_instalación_agente*`/`*arqu*`/qi/bin`

   donde:
   - *dir_instalación_agente* es el directorio de instalación de agente. El valor predeterminado es `C:\IBM\APM` en sistemas Windows y `/opt/ibm/apm/agent` en sistemas Linux y AIX.
   - *arqu* es el código de arquitectura de la plataforma. Por ejemplo, lx8266 representa Linux Intel v2.6 (64 bits). Para obtener una lista completa de los códigos de arquitectura, consulte el archivo *dir_instalación_agente*`/archdsc.tbl`.
2. Ejecute el script **`configDC`** para eliminar la biblioteca de salida de usuario de forma interactiva:
   - Windows

     ```
     configDC.bat –disable dir_instalación_iib
     ```
   - Linux AIX

     ```
     ./configDC.sh –disable dir_instalación_iib
     ```

   Donde *dir_instalación_iib* es el directorio de instalación de IBM Integration Bus.

Ejemplo

En el ejemplo siguiente se elimina la salida de usuario proporcionada por el agente para los intermediarios de la versión 9.0 instalados en un sistema AIX:

```
cd /opt/IBM/ITM/aix513/qi/bin
./configDC.sh –disable /opt/IBM/mqsi/9.0
```

Configuración de la supervisión de IBM MQ Appliances

El Agente de MQ Appliance es un agente de varias instancias. Tras la instalación, para poder iniciar la supervisión con el agente, primero debe configurar el agente creando una instancia del agente.

Antes de empezar

- Las instrucciones siguientes son para el release más reciente del agente, a excepción de lo indicado.

Procedimiento

- En los sistemas Linux y UNIX, puede configurar el agente con el script de configuración que solicita las respuestas o el archivo de respuestas silencioso.
  - "Configuración del agente respondiendo a solicitudes" en la página 302
  - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 303
- En los sistemas Windows, puede configurar el agente sólo con el archivo de repuestas silencioso.
  - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 303

Qué hacer a continuación

En la Consola de Cloud APM, vaya a Application Performance Dashboard para ver los datos recopilados. Para obtener más información sobre la utilización de la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si no puede ver los datos en los paneles de instrumentos del agente, consulte primero los registros de conexión del servidor y, a continuación, los registros del proveedor de datos. Las vías de acceso a estos registros se listan aquí:

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Configuración del agente respondiendo a solicitudes

Debe asignar primero un nombre de instancia a Agente de MQ Appliance y configurar el agente para poder iniciar la supervisión de IBM® MQ Appliances.

Procedimiento

Para configurar el agente mediante la ejecución del script y las respuestas a las solicitudes, siga estos pasos:

1. Ejecute el mandato siguiente:

   ```
   dir_instalación/bin/mq_appliance-agent.sh config nombre_instancia
   ```

   donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

   Ejemplo:

   ```
   /opt/ibm/apm/agent/bin/mq_appliance-agent.sh config AQM904
   ```

2. Responda a las solicitudes para establecer valores de configuración para el agente.

   Consulte la sección "Parámetros de configuración para el Agente de MQ Appliance" en la página 304 para obtener una descripción de cada uno de los parámetros de configuración.
3. Ejecute el mandato siguiente para iniciar el agente:

   ```
   dir_instalación/bin/mq_appliance-agent.sh start nombre_instancia
   ```

   Ejemplo:

   ```
   /opt/ibm/apm/agent/bin/mq_appliance-agent.sh start AQM904
   ```

Resultados

Ahora puede iniciar la sesión en la consola de Cloud APM y utilizar el editor de aplicaciones para añadir la instancia de Agente de MQ Appliance al Panel de instrumentos del rendimiento de aplicaciones. Si desea instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM"

en la página 1009. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte "Gestión de aplicaciones" en la página 1133.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

Para configurar el agente mediante la edición del archivo de respuestas silenciosas y la ejecución del script sin interacción, siga estos pasos:

1. Abra el archivo `mq_appliance_silent_config.txt` en uno de los siguientes directorios en un editor de texto.
   - Linux AIX *dir_instalación*`/samples/mq_appliance_silent_config.txt`
   - Windows *dir_instalación*`\samples\mq_appliance_silent_config.txt`

   donde *dir_instalación* es el directorio de instalación del agente. Por ejemplo, `/opt/ibm/apm/agent`.
2. En el archivo `mq_appliance_silent_config.txt` especifique valores para todos los parámetros obligatorios y modifique los valores predeterminados de otros parámetros según sea necesario.

   Consulte la sección "Parámetros de configuración para el Agente de MQ Appliance" en la página 304 para obtener una descripción de cada uno de los parámetros de configuración.
3. Guarde y cierre el archivo `mq_appliance_silent_config.txt` y ejecute el mandato siguiente:
   - Linux AIX

     ```
     dir_instalación/bin/mq_appliance-agent.sh config nombre_instancia
     vía_acceso_archivo_silencioso
     ```
   - Windows

     ```
     dir_instalación\bin\mq_appliance-agent.bat config nombre_instancia
     vía_acceso_archivo_silencioso
     ```

   donde:
   - *nombre_instancia* es el nombre que desea proporcionar a la instancia del agente. Por ejemplo, `AQM904`.
   - *vía_acceso_archivo_silencioso* es la vía de acceso al archivo `mq_appliance_silent_config.txt`. Por ejemplo, `/opt/ibm/apm/agent/samples/mq_appliance_silent_config.txt`.
4. Una vez completada la configuración, ejecute el mandato siguiente para iniciar el agente:
   - Linux AIX

     ```
     dir_instalación/bin/mq_appliance-agent.sh start nombre_instancia
     ```
   - Windows

```
dir_instalación\bin\mq_appliance-agent.bat start nombre_instancia
```

Resultados

Ahora puede iniciar la sesión en la consola de Cloud APM y utilizar el editor de aplicaciones para añadir la instancia de Agente de MQ Appliance al Panel de instrumentos del rendimiento de aplicaciones. Si desea instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte "Gestión de aplicaciones" en la página 1133.

Parámetros de configuración para el Agente de MQ Appliance

Los parámetros de configuración para el Agente de MQ Appliance se visualizan en tablas que los agrupan por secciones.

- Tabla 24 en la página 304: Propiedades para la recepción de sucesos SNMP y la decodificación de sucesos V3.
- Tabla 25 en la página 305: Propiedades para los valores de Java.
- Tabla 26 en la página 305: Propiedades para el servidor proxy utilizado por los proveedores HTTP.
- Tabla 27 en la página 306: Propiedades para el servidor HTTP.
- Tabla 28 en la página 306: Propiedades para la conexión al dispositivo MQ.

Tabla 24. Parámetros de configuración de sucesos SNMP

Nombre de parámetro	**Descripción**	**Nombre de parámetro en el archivo de configuración silenciosa**
Número de puerto	Número de puerto utilizado para la escucha de sucesos SNMP. El valor predeterminado es 162.	KQZ_SNMPEVENT_PORT
Nivel de seguridad	Nivel de seguridad utilizado para la conexión al suceso SNMP. Puede ser uno de lo valores siguientes: • 1=noAuthNoPriv • 2=authNoPriv • 3=authPriv El valor predeterminado es 2.	KQZ_SNMPEVENT_ SECURITY_LEVEL
Nombre de usuario	Nombre de usuario utilizado para la conexión al agente SNMP.El valor predeterminado es `snmpuser`.	KQZ_SNMPEVENT _USER_NAME
Protocolo aut.	Protocolo de autenticación utilizado para la conexión al agente SNMP. Puede ser uno de lo valores siguientes: • 1=MD5 • 2=SHA El valor predeterminado es 2.	KQZ_SNMPEVENT_AUTH _PROTOCOL

Tabla 24. Parámetros de configuración de sucesos SNMP (continuación)		
Nombre de parámetro	**Descripción**	**Nombre de parámetro en el archivo de configuración silenciosa**
Contraseña aut.	Contraseña de autorización utilizada para la conexión al agente SNMP.	KQZ_SNMPEVENT_AUTH _PASSWORD
Contraseña priv.	Contraseña de privacidad utilizada para la conexión al agente SNMP.	KQZ_SNMPEVENT_PRIV _PASSWORD
Archivo de configuración de condiciones de excepción	Ubicación del archivo de configuración de condiciones de excepción.	KQZ_SNMPEVENT_ TRAPCNFG_FILE

Tabla 25. Parámetros de configuración de Java		
Nombre de parámetro	**Descripción**	**Nombre de parámetro en el archivo de configuración silenciosa**
Nivel de rastreo de Java	Nivel de rastreo que utilizan los proveedores de Java. Puede ser uno de lo valores siguientes: • 1=Off • 2=Error • 3=Warning • 4=Information • 5=Minimum Debug • 6=Medium Debug • 7=Maximum Debug • 8=All El valor predeterminado es 2.	JAVA_TRACE _LEVEL

Tabla 26. Parámetros de configuración del servidor proxy		
Nombre de parámetro	**Descripción**	**Nombre de parámetro en el archivo de configuración silenciosa**
Nombre de host de proxy	Nombre de host del servidor proxy.	KQZ_HTTP _PROXY_HOSTNAME
Puerto de proxy	Número de puerto del servidor proxy. El valor predeterminado es 80.	KQZ_HTTP_PROXY_PORT
Nombre de usuario de proxy	Nombre de usuario para el servidor proxy.	KQZ_HTTP _PROXY_USER
Contraseña de proxy	Contraseña para el servidor proxy.	KQZ_HTTP _PROXY_PASSWORD

Tabla 27. Parámetros de configuración del servidor HTTP		
Nombre de parámetro	**Descripción**	**Nombre de parámetro en el archivo de configuración silenciosa**
Nombre de usuario HTTP	Nombre de usuario para acceder a la interfaz de gestión REST de MQ Appliance.	KQZ_HTTP _USER
Contraseña HTTP	Contraseña para acceder a la interfaz de gestión REST de MQ Appliance.	KQZ_HTTP _PASSWORD
Validación de certificados habilitada	Indica si se habilita la validación de certificados. Puede ser uno de lo valores siguientes: • 1=true • 2=false El valor predeterminado es 2.	KQZ_HTTP_CERTIFICATE _VALIDATION

Tabla 28. Parámetros de configuración de la conexión de dispositivo MQ		
Nombre de parámetro	**Descripción**	**Nombre de parámetro en el archivo de configuración silenciosa**
Host o dirección IP del dispositivo	Nombre de host o dirección IP del dispositivo MQ. El valor predeterminado es `https://hostnameoripaddress:` `https://9.123.123.123`.	KMK_APPLIANCE _HOST_OR _IP_ADDRESS.arm1
Número de puerto del dispositivo	Número de puerto de la conexión HTTPS al dispositivo MQ. El valor predeterminado es 5554.	KMK_APPLIANCE _PORT_NUMBER.arm1
Nombre de usuario del dispositivo	Nombre de usuario utilizado para la conexión al dispositivo MQ.	KMK_APPLIANCE _USER_NAME.arm1
Contraseña del usuario del dispositivo	Contraseña del usuario del dispositivo MQ.	KMK_APPLIANCE _USER_PASSWORD.arm1
Identificación de host del agente	Nombre de host del sistema donde se ejecuta el Agente de MQ Appliance. El valor predeterminado es `9.123.123.111`.	KMK_APM_ AGENT_IDENTIFICATION .arm1
Validación de certificados habilitada	Indica si se habilita la validación de certificados para la conexión HTTP. • 1=true • 2=false El valor predeterminado es 2.	KMK_CERTIFICATE _VALIDATION_ ENABLED.arm1

Configuración de la supervisión de InfoSphere DataStage

Debe configurar el Agente de DataStage para que el agente pueda recopilar datos para supervisar el estado y el rendimiento de los recursos del servidor DataStage.

Antes de empezar

Revise los requisitos previos de hardware y software, consulte Software Product Compatibility Reports para el agente de DataStage

Acerca de esta tarea

El Agente de DataStage es un agente de múltiple instancia. Deberá crear la primera instancia e iniciar el agente manualmente.

La versión del producto y la versión del agente a menudo difieren. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Configuración del agente en sistemas Windows

Puede utilizar la ventana de IBM Cloud Application Performance Management para configurar el agente en sistemas Windows.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Plantilla** en la columna **Tarea/Subsistema** y pulse **Configurar utilizando los valores predeterminados**.

   Se abrirá la ventana **Monitoring Agent for DataStage**.
3. En el campo **Especificar un nombre de instancia exclusivo**, escriba el nombre de una instancia del agente y pulse **Aceptar**.
4. En la ventana **Monitoring Agent for DataStage**, especifique valores para los parámetros de configuración y pulse **Aceptar**.

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 309.
5. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la instancia del agente que ha creado y pulse **Inicio** para iniciar el agente.

Configuración del agente en sistemas Linux

Para configurar el agente en sistemas operativos Linux, debe ejecutar el script y responder a las solicitudes.

Procedimiento

1. En la línea de mandatos, cambie la vía de acceso al directorio de instalación de agente.
   Ejemplo: `/opt/ibm/apm/agent/bin`
2. Ejecute el mandato siguiente, donde nombre_instancia es el nombre que asignará a la instancia:
   `./datastage-agent.sh config` *`nombre_instancia`*
3. Cuando la línea de mandatos muestre el siguiente mensaje, escriba 1 y especifique:

   `¿Editar valor de 'Monitoring Agent for DataStage'? [1=Sí, 2=No]`
4. Especifique valores para los parámetros de configuración cuando se le solicite.

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 309.

5. Ejecute el mandato siguiente para iniciar el agente:

   `./datastage-agent.sh start` *nombre_instancia*

Configuración de variables de entorno

Puede configurar variables de entorno para cambiar el comportamiento de Agente de DataStage .

Procedimiento

1. Abra el siguiente archivo en un editor de texto:
   a) Windows *dir_instalación*\TMAITM6_x64\KDTENV_*nombre_instancia*
   b) Linux *dir_instalación*/config/.dt.environment
2. Edite las siguientes variables de entorno:
   - **KDT_FIRST_COLLECTION_INTERVAL**: Intervalo de tiempo en segundos de la primera recopilación de datos. Establezca este intervalo de tiempo en un periodo durante el que el agente recopilará los datos de ejecuciones de trabajos anteriores en el tiempo especificado hasta que se inicia el agente. El valor predeterminado es 300 segundos (5 minutos). Por lo tanto, si el agente se inicia a las 14:00, recopila los datos de ejecuciones de trabajos desde las 13:55 hasta las 14:00. Esto sirve para evitar la tormenta de datos de ejecuciones de trabajos históricos cuando el agente empieza a recopilar datos. Todas las recopilaciones de datos de agente subsiguientes para ejecuciones de trabajos captan solo las ejecuciones de trabajos recién añadidas que tuvieron lugar desde la última recopilación.
   - **KDT_SSL_CONTEXT**: Protocolo SSL que está habilitado en el nivel de servicios (WebSphere Application Server). El valor predeterminado es TLS.
   - **KDT_META_SCHEMA_NAME**: Nombre del esquema de base de datos que se crea para el repositorio de metadatos. El valor predeterminado es DSODB para Db2 y xmeta para bases de datos MSSQL y Oracle.
   - **KDT_DATABASE_SERVICE_NAME**: Nombre de base de datos o servicio que utiliza el agente para conectarse al repositorio de metadatos. El valor predeterminado es XMETA para Db2, xmeta para MSSQL y ORCL para bases de datos Oracle.
   - **KDT_DISABLED_ATTRIBUTEGROUP**: Lista separada por comas de grupos de atributos cuya recopilación de datos debe estar no disponible. Los siguientes valores se pueden establecer como únicos o varios para el respectivo grupo de atributos: JobRuns, JobProperties, JobRunLog, JobStages, JobParameters, EngineSystemConfiguration, EngineSystemResources, EngineServiceStatus, EngineStatusSummary, JobActivity, AgentConfiguration y JobConfiguration.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

Puede utilizar el archivo de respuestas silencioso para configurar el Agente de DataStage en el sistema Linux y Windows. Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

1. En un editor de texto, abra el archivo de configuración silencioso que está disponible en la siguiente ubicación y especifique valores para todos los parámetros:

   Windows *dir_instalación*\samples\datastage_silent_config.txt

Linux *dir_instalación*\samples\datastage_silent_config_UNIX.txt

Windows C:\IBM\APM\samples

Linux /opt/ibm/apm/agent/samples

Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 309.

2. En la línea de mandatos, cambie la vía de acceso a *dir_instalación*\bin.
3. Ejecute el mandato siguiente:

   Windows `datastage-agent.bat config` *nombre_instancia dir_instalación* `\samples\datastage_silent_config.txt`

   Linux `datastage-agent.sh config` *nombre_instancia dir_instalación*`\samples\datastage_silent_config_UNIX.txt`
4. Inicie el agente.

   Windows En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón la instancia de agente que ha creado y pulse **Iniciar**.

   Linux Ejecute el mandato siguiente: `./datastage-agent.sh start` *nombre_instancia*

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Parámetros de configuración del agente

Al configurar el Agente de DataStage , puede cambiar los parámetros de nivel de servicios, repositorio de metadatos y los parámetros de configuración avanzada.

Parámetros de configuración del nivel de servicios

Los parámetros de configuración que son necesarios para que el agente se conecte al nivel de servicios.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del nivel de servicios del Agente de DataStage .

Tabla 29. Nombres y descripciones de los parámetros de configuración del nivel de servicios

Nombre de parámetro	Descripción	Campo obligatorio
Nombre del host	Nombre de host del sistema donde está instalado el nivel de servicios. Si el sistema forma parte de un dominio, especifique el nombre de dominio completo (FQDN). El valor predeterminado es localhost.	Sí
Puerto HTTPS	Puerto HTTPS para la interfaz REST en el sistema donde está instalado el nivel de servicios. El valor predeterminado es 9443.	Sí
Nombre de usuario de WAS	El nombre de usuario para conectarse a WebSphere Application Server. El valor predeterminado es wasadmin.	Sí
Contraseña de WAS	La contraseña para conectarse a WebSphere Application Server.	Sí
Confirmar contraseña de WAS	La contraseña que se ha especificado en el campo **Contraseña de WAS**.	Sí

Parámetros de configuración del repositorio de metadatos

Los parámetros de configuración que son necesarios para que el agente se conecte al repositorio de metadatos.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del repositorio de metadatos del Agente de DataStage .

Tabla 30. Nombres y descripciones de los parámetros de configuración del repositorio de metadatos

Nombre de parámetro	Descripción	Campo obligatorio
Tipo de base de datos	Tipo de base de datos del repositorio de metadatos. Db2El valor predeterminado es 1.	Sí
Nombre del host	Nombre de host del sistema donde está instalado el repositorio de metadatos. Si el sistema forma parte de un dominio, especifique el nombre de dominio completo (FQDN). El valor predeterminado es localhost.	Sí
Puerto de base de datos	Puerto de base de datos del repositorio de metadatos para la conexión JDBC. El valor predeterminado es 50000.	Sí
Nombre de usuario de base de datos	El nombre de usuario para conectarse a la base de datos de operaciones. El valor predeterminado es dsodb.	Sí
Contraseña de la base de datos	La contraseña para conectarse a la base de datos de operaciones.	Sí
Confirmar contraseña de la base de datos	La contraseña que se ha especificado en el campo **Contraseña de base de datos**.	Sí
Vía de acceso de controlador JDBC	Vía de acceso al controlador JDBC incluido el archivo jar. Por ejemplo, /home/jars/db.jar en Linux.	Sí

Parámetros de configuración avanzada

Tabla 31. Nombres y descripciones de los parámetros de configuración avanzada

Nombre de parámetro	Descripción	Campo obligatorio
Nivel de rastreo de Java	Los niveles de rastreo que utilizan los proveedores personalizados de Java. El valor predeterminado es 2.	Sí

Parámetros de configuración del cliente de API Java

Tabla 32. Nombres y descripciones de los parámetros de configuración del cliente de API Java

Nombre de parámetro	Descripción	Campo obligatorio
Vía de acceso de clases para los jar externos		No

Configuración de Internet Service Monitor

El agente de Internet Service Monitoring ofrece la capacidad de determinar si un servicio concreto funciona correctamente, identificar áreas de problemas y notificar el rendimiento de servicio medido en relación con los acuerdos de nivel de servicio. Agente de Internet Service Monitoring funciona emulando

las acciones de un usuario real. Sondea o prueba periódicamente los servicios de Internet para comprobar su estado y rendimiento.

Visión general

Al supervisar servicios de Internet, se define qué es lo que se va a supervisar, para quién y cuándo. Puede configurar los supervisores mediante la interfaz de usuario de configuración de Agente de Internet Service Monitoring.

El supervisor prueba servicios de Internet específicos y reenvía los resultados de las pruebas a Databridge. Los supervisores emulan las acciones de un usuario real del servicio.

Por ejemplo, el supervisor HTTP intenta periódicamente acceder a una página web emulando las solicitudes que un navegador web suele enviar cuando un usuario va a la página. El supervisor registra el resultado de la prueba, que se envía a Databridge.

Internet Service Monitoring

Cada supervisor se ha diseñado para probar un tipo de protocolo o servicio. Por ejemplo, el supervisor HTTP prueba la disponibilidad de recursos como, por ejemplo, páginas web a través del protocolo Hypertext Transfer Protocol, y el supervisor FTP prueba la transferencia de archivos entre hosts que ejecutan el protocolo de transferencia de archivos.

Un supervisor puede probar muchas instancias diferentes del mismo servicio como, por ejemplo, una serie de páginas web servidas por un rango de hosts.

Supervisión de servicios web

Utilizando el rango de supervisores de la supervisión de servicios de Internet, puede adaptar el tipo de supervisión de servicios web que proporciona desde la supervisión de servicios de Internet básicos que prueba la disponibilidad de una página web, hasta la combinación de secuencias de pruebas.

La supervisión de servicios de Internet utiliza un sondeo de gran volumen y de baja complejidad para probar la disponibilidad de los servicios web. Por ejemplo, si desea supervisar la disponibilidad general de un sitio web, podría utilizar el supervisor HTTP para sondear muchos URL a intervalos regulares.

Utilizando una combinación de supervisores, puede crear un nivel de supervisión de servicios apropiado para sus requisitos:

- Supervisores HTTP y HTTPS

  Supervise la disponibilidad de recursos a través de HTTP o HTTPS ejecutando pruebas básicas de una sola solicitud con un gran volumen.
- Supervisor de transacciones (TRANSX)

  Combine secuencias de pruebas realizadas por un grupo de supervisores, que simulan la acciones de un usuario real. Por ejemplo, marcar un servicio, acceder a un número de páginas de varios sitios web y después acceder a servicios de correo electrónico.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte “Historial de cambios” en la página 52.

Configuración de Internet Service Monitoring a través de la interfaz de usuario

Para supervisar servicios de Internet, cree perfiles de usuario, elementos de perfil y planificaciones de supervisión. Configure perfiles de usuario, elementos de perfil y planificaciones de supervisión utilizando la interfaz de usuario de Internet Service Monitoring.

Acerca de esta tarea

Un perfil de usuario es un cliente, o un departamento, o un grupo de servicios para los cuales se supervisan servicios de Internet o servicios web. Para cada perfil de usuario, el usuario necesita definir uno o más elementos de perfil. Por ejemplo, el usuario podría definir un elemento de perfil para supervisar una página web entregada a través de un servicio HTTP, o un elemento de perfil para supervisar la disponibilidad de un servicio FTP. Los perfiles de usuario normalmente contienen varios elementos de perfil, cada elemento de perfil prueba uno de los servicios proporcionados a ese usuario. Cada perfil de usuario también tiene una planificación de supervisión asociada que determina en qué día y a qué hora se van a ejecutar las pruebas definidas en el perfil.

Para acceder a la ventana de configuración del agente de Internet Service Monitoring a través del panel de instrumentos de IBM Application Performance Management, utilice el siguiente método:

Procedimiento

1. En el panel de instrumentos de Application Performance Management, pulse el icono  . Pulse **Configuración de agente**,

   Se abre la ventana de configuración de agente.
2. Pulse la pestaña **ISM** para configurar el agente de Internet Service Monitoring.

   Puede crear, editar, suprimir, renovar, planificar y filtrar los perfiles de usuario. Despliegue los perfiles de usuario creados en el sistema gestionado seleccionado. La versión visualizada es la versión del sistema gestionado. El nombre de perfil indica el perfil de usuario desplegado en los sistemas gestionados seleccionados. Siga estos pasos para configurar cualquiera de los perfiles y realizar el despliegue en los sistemas gestionados.
3. Para añadir un perfil, pulse el icono  . Escriba el **Nombre de perfil** y la **Descripción** en el recuadro de diálogo.
4. Pulse **Siguiente**.
5. Seleccione un supervisor en la lista desplegable de supervisores y pulse **Siguiente**.
6. Proporcione los valores de los campos y pulse **Añadir**.

   Se pueden seleccionar varios supervisores para un perfil. Consulte “Supervisores de Internet Service Monitoring disponibles” en la página 315 para ver los supervisores disponibles.
7. Pulse **Realizado**.
8. Pulse el icono  .
9. En el campo **Filtro**, busque los perfiles de usuario por su nombre.
10. Para desplegar el perfil que ha creado en un sistema gestionado, marque el recuadro de selección de los perfiles creados que deben configurarse y seleccione un sistema gestionado. Pulse **Desplegar** para desplegar el perfil en el nombre del sistema gestionado seleccionado.

Edición del perfil

Todos los perfiles de usuario que se crean son editables.

Acerca de esta tarea

Utilice el siguiente procedimiento para editar los perfiles.

Procedimiento

1. Seleccione **nombre de perfil** y pulse  .
2. Seleccione un servicio para editarlo y pulse **Editar**.

   a. Añada un supervisor utilizando el icono  y suprima el supervisor utilizando

   b. Para renombrar un perfil, efectúe una doble pulsación en el campo de texto **Nombre de perfil**, modifique el nombre del perfil y pulse **Renombrar perfil**.

3. Edite los valores del servicio seleccionado.

   Nota:

   - Para habilitar el campo de contraseña para editarlo, efectúe una doble pulsación en el campo de texto **username**. El usuario puede editar o añadir un nombre de usuario, y cambiar la contraseña.
   - Para habilitar el campo **sslkeypassword** para editarlo, efectúe una doble pulsación en su texto para cambiar la clave secreta.

4. Pulse **Guardar** y pulse el icono para renovar.

Planificación de un perfil
Los perfiles que se crean se pueden planificar para desplegarse en una fecha y hora determinadas.

Acerca de esta tarea

Utilice el siguiente procedimiento para planificar perfiles.

Procedimiento

1. Seleccione **nombre de perfil**.
2. Pulse el botón **Planificar**.
3. Planifique el perfil seleccionando el día y la hora. El usuario puede arrastrar la cuadrícula para seleccionar la hora que desea.
4. Pulse **Guardar**.
5. Pulse el icono para renovar.

Supresión de un perfil
Los perfiles que se crean se pueden suprimir permanentemente.

Acerca de esta tarea

Utilice el siguiente procedimiento para suprimir los perfiles.

Procedimiento

1. Seleccione **nombre perfil**.
2. Pulse el icono para suprimir el perfil.

Grupos de OID
Los grupos de OID (identificador de objeto) son parámetros específicos de supervisor opcionales. Definen conjuntos de uno o más OID de los objetos de la Base de información de gestión (MIB) de un dispositivo. El supervisor SNMP utiliza los grupos de OID para recuperar datos de esos objetos MIB cuyos OID aparecen en un grupo de OID especificado.

Los detalles de los objetos MIB desde los cuales el supervisor extrae datos son estos:

- Valor de OID

  El identificador numérico de la instancia del objeto MIB expresado en notación ASN.1, por ejemplo `.1.3.6.1.2.1.1.2.0`, o el nombre del objeto, por ejemplo `sysObjectID.0`

  Nota: Cuando se utiliza la notación ASN.1, debe incluir el carácter `.` inicial en el OID.

  Nota: Sólo puede utilizar un nombre de instancia de objeto para especificar el valor OID si el documento MIB que define el nombre es accesible para el supervisor. El directorio predeterminado para los documentos MIB es `$ISHOME/mibs`.

- Nombre de OID

  El nombre del objeto MIB, por ejemplo `sysObjectID`. Este nombre se utiliza en las clasificaciones de niveles de servicios y en los elementos de supervisor `$oidName`*n*.

- Unidad de OID

  Las unidades de los datos que contiene el objeto MIB. Por ejemplo, segundos, bytes o bits por segundo (BPS). Establézcala en BPS para habilitar el cálculo de bits por segundo para el OID. Los valores de bits por segundo se calculan como:

  ```
  (valor_sondeo_actual - valor_sondeo_anterior) / intervalo_sondeo* 8
  ```

- Selector

  El valor de índice del objeto MIB. La tabla siguiente muestra un ejemplo que lleva a que el selector busque en todas las filas `ifDescr` el valor `FastEthernet0/1`, dando un índice de fila de 2. A continuación, se consulta la fila `ifPhysAddress.2` y se devuelve el valor `0:6:53:34:d2:a1`. De esta manera, el índice 2 no se especifica directamente, de manera que si el índice para `FastEthernet0/1` cambia, no es necesario volver a configurar los grupos de OID.

Tabla 33. Utilización del valor de índice

Objeto MIB	**Valor del objeto MIB**
Valor de OID	`ifPhysAddress`
Nombre de OID	`FastEthernet0/1PhysicalAddress`
Unidad de OID	`serie`
Selector	`ifDescr=FastEthernet0/1`

Creación de un grupo de OID y un objeto MIB

Los grupos de OID se crean globalmente y pueden ser utilizados por todos los perfiles de usuario que supervisan dispositivos habilitados para SNMP.

Procedimiento

Siga estos pasos para crear un grupo de OID y un objeto MIB.

1. Pulse el botón **OIDs** para crear un grupo de OID en el panel de instrumentos de Internet Service Monitoring Agent.
2. Pulse el icono ⊕ y especifique el nombre del grupo de OID en el campo **Nombre de grupo de OID**.
3. Pulse el icono ⊕ para añadir el objeto MIB.
   a. Especifique el **valor**, el **Nombre**, la **Unidad** y el **selector** para el objeto MIB.
   b. Pulse **Añadir**.

   El objeto MIB se ha creado satisfactoriamente.
4. Pulse el icono ↻ para renovar.
   El grupo de OID se ha creado satisfactoriamente
5. Seleccione un **Nombre de grupo de OID** y pulse **Ver** para ver la lista de todos los objetos MIB creados bajo el **Grupo de OID**seleccionado.
6. Pulse **Cerrar**.

Edición de grupo de OID y objeto de MIB

Puede editar los grupos de OID. Los objetos MIB también se pueden editar al crear el grupo de OID o después de crear el grupo de OID.

Procedimiento

Siga estos pasos para editar un grupo de OID.

1. Pulse el botón **OID** para editar un grupo de OID en el panel de instrumentos de Internet Service Monitoring Agent.

2. Seleccione el nombre de grupo de OID en la lista **Nombre de grupo de OID** y pulse el icono .
3. Seleccione el valor en **Editar grupo de OID** y pulse el icono .
4. Modifique los campos de objeto de MIB de acuerdo con los requisitos y pulse el botón **Guardar**.
5. Pulse **Guardar** en la página emergente **Grupos de OID**.
6. Pulse **Cerrar**.

Supresión de un grupo de OID

Los objetos MIB se encuentran en grupos de OID y los utiliza el supervisor de SNMP para obtener datos. Puede suprimir objetos MIB individuales de un grupo de OID, o bien, puede suprimir todos los MIB al suprimir el grupo de OID completo.

Procedimiento

Siga estos pasos para suprimir un grupo de OID.

1. Para suprimir el grupo de OID, pulse el botón **OID** en el panel de instrumentos de Internet Service Monitoring Agent.
2. Seleccione el nombre de grupo de OID en la lista **Nombre de grupo de OID** y pulse el icono .
   Se suprimirá el grupo de OID junto con el objeto MIB.
3. Pulse **Cerrar**.

Supresión de un objeto MIB

Procedimiento

Siga estos pasos para suprimir el objeto MIB.

1. Para suprimir el objeto MIB, pulse el botón **OID** en el panel de instrumentos de Internet Service Monitoring Agent.
2. Seleccione el nombre de grupo de OID en la lista **Nombre de grupo de OID** y pulse el icono .
3. Seleccione el valor del objeto MIB y pulse el icono .
   El objeto MIB se suprimirá.
4. Pulse **Guardar** en la página emergente **Editar grupo de OID**.
5. Pulse **Cerrar**.

Supervisores de Internet Service Monitoring disponibles

El Agente de Internet Service Monitoring es un conjunto de supervisores que abarca una amplia gama de servicios de Internet.

La siguiente tabla lista los supervisores disponibles en el Agente de Internet Service Monitoring y los tipos de servicios que supervisa.

Tabla 34. Supervisores de servicios de Internet disponibles

Nombre del supervisor	**Tipo de servicio supervisado**
DHCP	Protocolo de configuración dinámica de host. Para configurar DHCP, consulte “Supervisor DHCP” en la página 329.
DNS	Sistema de nombres de dominio. Para configurar DNS, consulte “Supervisor DNS ” en la página 331.
FTP	Protocolo de transporte de archivos. Para configurar FTP, consulte “Supervisor FTP” en la página 336.

Tabla 34. Supervisores de servicios de Internet disponibles (continuación)	
Nombre del supervisor	**Tipo de servicio supervisado**
HTTP	Protocolo de transporte de hipertexto. Para configurar HTTP, consulte “Supervisor HTTP ” en la página 341 .
HTTPS	Protocolo de transporte de hipertexto (seguro). Para configurar HTTPS, consulte “Supervisor HTTPS” en la página 351.
ICMP	Protocolo de control de mensajes de Internet. Para configurar ICMP, consulte “Supervisor ICMP ” en la página 357.
LDAP	Lightweight Directory Access Protocol. Para configurar LDAP, consulte “Supervisor LDAP” en la página 362.
IMAP4	Protocolo de acceso a mensajes de Internet. Para configurar IMAP4, consulte “Supervisor IMAP4 ” en la página 368.
NTP	Protocolo de hora de red. Para configurar NTP, consulte “Supervisor NTP” en la página 373.
NNTP	Network News Transport Protocol. Para configurar NNTP, consulte “Supervisor NNTP” en la página 376.
POP3	Protocolo de oficina de correo. Para configurar POP3, consulte “Supervisor POP3” en la página 382.
RADIUS	Servicio del usuario de marcación de autenticación remota (Remote Authentication Dial-In User Service). Para configurar RADIUS, consulte “Supervisor RADIUS” en la página 387.
RPING	Ping remoto (Cisco, Juniper y RFC2925). Para configurar RPING, consulte “Supervisor RPING” en la página 392.
RTSP	Protocolo de modalidad continua en tiempo real. Para configure RTSP, consulte “Supervisor RTSP” en la página 398.
SAA	Cisco Service Assurance Agent. Para configurar SAA, consulte “Supervisor SAA” en la página 405.
SIP	Protocolo de iniciación de sesiones. Para configurar SIP, consulte “Supervisor SIP” en la página 421
SMTP	Protocolo de transporte de correo simple. Para configurar SMTP, consulte “Supervisor SMTP” en la página 426.

Tabla 34. Supervisores de servicios de Internet disponibles (continuación)	
Nombre del supervisor	**Tipo de servicio supervisado**
SNMP	Protocolo simple de gestión de red. Para configurar SNMP, consulte "Supervisor SNMP" en la página 430.
SOAP	Protocolo de mensajería basado en XML. Para configurar SOAP, consulte "Supervisor SOAP" en la página 435.
TCPPort	Protocolo de control de transmisión. Para configurar TCPPort, consulte "Supervisor TCPPort " en la página 440
TFTP	Trivial File Transfer Protocol. Para configurar TFTP, consulte "Supervisor TFTP" en la página 444.
TRANSX	Transacciones. Para configurar TRANSX, consulte "Supervisor TRANSX" en la página 450.

Archivos

Archivo ejecutable

Cada supervisor de servicios de Internet consta de un archivo ejecutable, un archivo de propiedades y un archivo de registro.

Los archivos ejecutables de supervisor se encuentran en el directorio `$ISHOME/platform/arch/bin`. El valor de `arch` es el código de arquitectura del sistema operativo Windows - `win 32`.

Archivo de propiedades

El archivo de propiedades es un archivo de texto e incluye valores predeterminados precedidos por el símbolo hash.

Para cambiar un valor, cambie el valor predeterminado y elimine el símbolo hash, o copie y pegue la línea que contiene los valores predeterminados, haga el cambio y elimine el símbolo hash. Esto permite restaurar más tarde los valores predeterminados. Los archivos de propiedades de supervisión se encuentran en el directorio `$ISHOME/etc/props`.

Archivo de reglas

Los archivos de reglas son parecidos a los archivos de reglas de analizador de IBM Application Performance Management Netcool/OMNIbus. Para obtener información sobre su sintaxis, consulte la publicación *IBM Application Performance Management Netcool/OMNIbus Probe and Gateway Guide*.

Los archivos de reglas del supervisor se encuentran en el directorio `$ISHOME/etc/rules`.

Archivo de registro

Los archivos de registro almacenan mensajes sobre el funcionamiento del supervisor.

Los archivos de reglas del supervisor se encuentran en el directorio `$ISHOME/log`. La propiedad `MessageLog` determina la ubicación y el nombre del archivo de registro. La propiedad `MessageLevel` selecciona el nivel de información que se graba en el archivo de registro, por ejemplo, mensajes de depuración detallados o mensajes de error irrecuperable. La propiedad `MaxLogFileSize` determina el tamaño del archivo de registro antes del reinicio.

El nombre predeterminado del archivo de registro es `nombre.log`, donde *nombre* es el nombre del supervisor.

Funciones comunes

Hay diversas funciones que son comunes a todos los supervisores de servicios de Internet. Estas características constan de propiedades, los resultados generados por supervisores y los mensajes de estado.

Esta sección describe las propiedades de todos los supervisore. Las propiedades específicas del supervisor se describen en las secciones de cada supervisor.

En la tabla siguiente, los parámetros de propiedad predeterminados se ponen de relieve cuando sea aplicable.

Tabla 35. Propiedades comunes

Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
AddRoute	0|1	Crea una ruta desde la dirección IP de la interfaz de red que utiliza el supervisor a la dirección IP del host supervisado. 0 - inhabilitado 1: habilitado (el supervisor utiliza la ruta especificada en el elemento de perfil, y no en otra interfaz de red). **Nota:** Esta propiedad no se admite en las plataformas AIX y HP-UX.
BridgeIPAddress	no aplicable	Especifica la dirección IP de Databridge. Esta propiedad no es configurable; Databridge está siempre en el host local.
BridgePort	entero	Número de puerto utilizado por Databridge. Configure en esta propiedad el mismo valor que en la propiedad SocketPort de Databridge. Valor predeterminado: 9510
BridgeSSLAuthenticatePeer	0|1	Si desea configurar la autenticación SSL entre el supervisor y el puente, o entre el puente y el agente, establezca BridgeSSLAuthenticatePeer en 1 y reinicie el puente. Esta acción autentica los certificados del servidor. Los certificados se almacenan en el BridgeSSLTrustStore. 0 - inhabilitado 1 - habilitado
BridgeSSLCertificateFile	serie	Especifica la vía de acceso y el nombre de archivo del certificado SSL de Bridge digital. Valor predeterminado: $ISHOME/certificates/monitorCert.pem

Tabla 35. Propiedades comunes (continuación)

Nombre de propiedad	Parámetro de propiedad	Descripción
BridgeSSLCipherSet	serie	Especifica un CipherSet. Si actualiza este valor, utilice la sintaxis de cifrado definida en la documentación de OpenSSL. **Nota:** Establezca el mismo valor en el agente de supervisión de servicios de Internet, en todos los supervisores y en Databridge. Valor predeterminado: RC4:3DES:DES:+EXP
BridgeSSLDisableSSLv2	0|1	Determina qué tipos de sockets se aceptan. • Si se establece en 0, se acepta SSLv2 y SSLv3. • Si se establece en 1, los sockets se abren sólo en SSLv3. **Restricción:** Establezca el mismo valor en el agente de supervisión de servicios de Internet, en todos los supervisores y en Databridge.
BridgeSSLEncryption	0|1	Habilita el cifrado SSL de Bridge. Configure en esta propiedad el mismo valor que en la propiedad de Databridge correspondiente. 0 - inhabilitado 1 - habilitado **Nota:** Configure el mismo valor para todos los supervisores.
BridgeSSLKeyFile	serie	La vía de acceso y el nombre de archivo del archivo de claves privadas SSL de Bridge. Valor predeterminado: $ISHOME/certificates/monitorKey.pem
BridgeSSLKeyPassword	serie	Contraseña que se utiliza para cifrar la clave privada SSL de Bridge. Valor predeterminado: tivoli

Tabla 35. Propiedades comunes (continuación)		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
`BridgeSSLTruststore`	serie	La vía de acceso y el nombre de archivo del archivo de certificado de confianza para la autenticación. Solo es necesario cuando se utiliza el parámetro `BridgeSSLAuthenticatePeer`. Si desea configurar la autenticación SSL entre el supervisor y el puente, o entre el puente y el agente, establezca `BridgeSSLAuthenticatePeer` en `1` y reinicie el puente. Esta acción autentica los certificados del servidor. Puede almacenar certificados en `SSLTrustStoreFile` y en `SSLTrustStorePath`. Valores predeterminados: • `SSLTrustStoreFile`, `$ISHOME/certificates/trust.pem` • `SSLTrustStorePath`, `$ISHOME/certificates/` Para añadir nuevos certificados, realice uno de los pasos siguientes: • Añada un certificado al final de la lista en el archivo de texto `SSLTrustStoreFile`. • Añada un certificado al directorio `SSLTrustStorePath` y ejecute el mandato OpenSSL `c_rehash` *`dir_certificado`* para realizar hash en los certificados.
`BridgeTimeout`	entero	Tiempo, en segundos, que el supervisor espera una respuesta de Databridge.
`ConfigFile`	serie	Utilícelo para apuntar a un archivo de configuración del supervisor. Valor predeterminado: en blanco (serie vacía).
`ConfigurationCheckInterval`	entero	Intervalo (en segundos) con el que el supervisor comprueba si se han realizado cambios en el perfil. Valor predeterminado: `1`
`Datalog`	`0`|`1`	Fuerza al supervisor a registrar los datos de rendimiento en un archivo de registro de datos. Los datos de rendimiento se registran en: `$ISHOME/datalogs/`*`perfil_usuario`* `0` - inhabilitado `1` - habilitado

Tabla 35. Propiedades comunes (continuación)

Nombre de propiedad	Parámetro de propiedad	Descripción
DatalogFormat	serie	Define el formato del archivo de registro de datos. El parámetro es una lista de elementos separados por espacios cuyos valores deben almacenarse en el archivo de registro de datos. Para cada resultado de sondeo escrito en el archivo de registro de datos, se registran la hora actual ($time) y el tiempo empleado ($totalTime), seguidos de todos los elementos definidos en esta propiedad.
DatalogNameFormat	serie	Formato del nombre de archivo del registro de datos.
Dominio	serie	Especifica el nombre de dominio del host que ejecuta el supervisor. Si esta propiedad no se establece, el supervisor intentará adivinar el nombre de dominio utilizando las configuraciones de NIS y DNS.
DumpProps	no aplicable	Muestra una lista de todas las propiedades de un supervisor.
FullHostInfo	0|1	Especifica si se va a correlacionar el elemento $host con un elemento de dirección IP $hostIP (si $host es un nombre de DNS) o con un elemento de nombre de DNS (si $host es una dirección IP). 0 - inhabilitado 1 - habilitado **Nota:** Esto no está disponible en el supervisor TRANSX.
GroupID	serie	El ID de grupo con el que deberá ejecutarse el supervisor.
Ayuda	0|1	Muestra la ayuda para las opciones de la línea de mandatos sin ejecutar el supervisor. 0 - inhabilitado 1 - habilitado
IdentifierChecksumFields	serie	En desuso.

Tabla 35. Propiedades comunes (continuación)		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
IgnoreUnmatchedDVC	0|1	Si una clasificación de niveles de servicios concreta no coincide (elemento no creado por el supervisor), omita ese elemento en el cálculo del nivel de servicios. **Consejo:** En versiones anteriores de Agente de Internet Service Monitoring, las clasificaciones de niveles de servicio se denominaban Discrete Value Classifications (DVC). 0 - inhabilitado 1 - habilitado
IpAddress	serie	Especifica la dirección IP de la interfaz de red que utiliza el supervisor durante las pruebas. Si esta propiedad no está configurada, el supervisor intenta determinar la dirección IP de la máquina host utilizando una búsqueda de nombre de host. Este intento puede fallar si la máquina host tiene más de una interfaz de red.
Manager	serie	Especifica el nombre de la aplicación de gestión, que se utiliza en la eliminación de duplicados del suceso ObjectServer.
MaxCCA	entero	Establece el número máximo de conexiones simultáneas que puede tener el supervisor en cualquier momento. Tenga en cuenta que si establece este valor demasiado alto, esto podría tener un efecto grave sobre el rendimiento del supervisor. Esta propiedad no está disponible para el supervisor ICMP. Valor predeterminado: 10
MaxLogFileSize	entero	El tamaño máximo (en bytes) del archivo de registro. Valor predeterminado: 1048576
MessageLevel	serie	El nivel inferior de mensajes que se van a enviar al registro de mensajes. Los valores, en orden descendente de gravedad, son estos: debug, info, warn, error y fatal. Valor predeterminado: warn
MessageLog	serie	Ubicación del archivo de registro. Valor predeterminado: $ISHOME/log/*supervisor*.log

Tabla 35. Propiedades comunes (continuación)

Nombre de propiedad	Parámetro de propiedad	Descripción
MinPoll	entero	Define el intervalo de sondeo mínimo permitido. Si alguno de los archivos de configuración del supervisor tiene un intervalo de sondeo establecido por debajo de este valor, el valor del archivo de configuración se sobrescribe. Valor predeterminado: 60
MsgDailyLog	entero	Habilita la generación de un archivo de registro diario. Valor predeterminado: 0: registro diario inhabilitado
MsgTimeLog	serie	Especifica la hora (en formato HHMM de 24 horas) tras la cual el supervisor genera un registro diario, si MsgDailyLog está habilitado. Valor predeterminado: 0000 - 12 medianoche
Nombre	serie	Nombre del supervisor. Establecer esta propiedad restablece las propiedades PropsFile, RulesFile y MessageLog en sus valores predeterminados.
NewProfileCheckMultiple	entero	Múltiplo que indica la frecuencia con la que el supervisor comprueba si hay nuevos archivos de configuración cuando busca cambios de perfil. Valor predeterminado: 10
NoRecover	entero	Indica al supervisor que no recupere el archivo de almacenamiento y reenvío. Valor predeterminado: 0 - la recuperación no se suprime
Pause	entero	Establece el intervalo (en segundos) en el que un supervisor genera hebras. Configurar valores más altos en esta propiedad, como 100 o más, fuerza al supervisor a generar hebras a una velocidad más lenta. Aumentar el valor suele ser necesario sólo en sistema lentos. Esta propiedad no se admite en el supervisor ICMP. Valor predeterminado: 50
PreviousFields	serie	Elementos especificados por esta propiedad (utilizando el formato "<elemento>, <elemento>, …") se almacenan para un solo sondeo y se les añade como prefijo la cadena previous.

Tabla 35. Propiedades comunes (continuación)

Nombre de propiedad	Parámetro de propiedad	Descripción
`Profile`	serie	Nombre del perfil del cliente, o los perfiles que se utilizará. La cadena puede ser un nombre de perfil único, una lista de nombres de perfil separados por espacios, o `*`, que fuerza al supervisor a utilizar todos los perfiles disponibles. Valor predeterminado: `*`
`ProfileUpdateTimeout`	entero	Número de milisegundos que un archivo de perfil debe permanecer estático antes de que pueda leerlo un supervisor y actualizarlo. El rango permisible es de `1-20000` milisegundos. Valor predeterminado: `100`
`PropsFile`	serie	Nombre del archivo de propiedades. Valor predeterminado: `$ISHOME/etc/props/`*`monitor`*`.props`
`QFile`	serie	Establece el nombre del archivo de almacenamiento y reenvío. Valor predeterminado: `$ISHOME/var/`*`monitor`*`.saf`.
`QSize`	entero	Establece el tamaño reservado (en bytes) del archivo de almacenamiento y reenvío. Valor predeterminado: `10240000`
`ID de usuario`	serie	ID de usuario con el que deberá ejecutarse el supervisor. **Nota:** No utilice esta propiedad con el supervisor DHCP.
`Versión`	no aplicable	Imprime la versión de supervisor sin ejecutar el supervisor.

Elementos comunes de supervisor

En esta sección se describen los elementos generados por todos los supervisores. Los elementos específicos de supervisor se describen en las secciones de supervisor individuales. Los elementos generados se pueden visualizar en el panel de instrumentos del agente de Internet Service Monitoring.

Si utiliza IBM Application Performance Management, los elementos que se pueden visualizar en el panel de instrumentos del agente como atributos los determina un archivo de correlación generado por el agente de supervisión de servicios de Internet. Este archivo de correlaciones no se puede configurar.

Tabla 36 en la página 325 lista los elementos generados por todos los supervisores. Los elementos indicados con un asterisco (*) están disponibles como atributos de espacio de trabajo. Los nombres de los atributos se muestran entre corchetes. La ausencia de un asterisco indica que no hay ningún atributo de espacio de trabajo equivalente. Los atributos que se muestran entre corchetes, pero sin un elemento indican que solo están disponibles como atributos de espacio de trabajo, no hay ningún elemento equivalente.

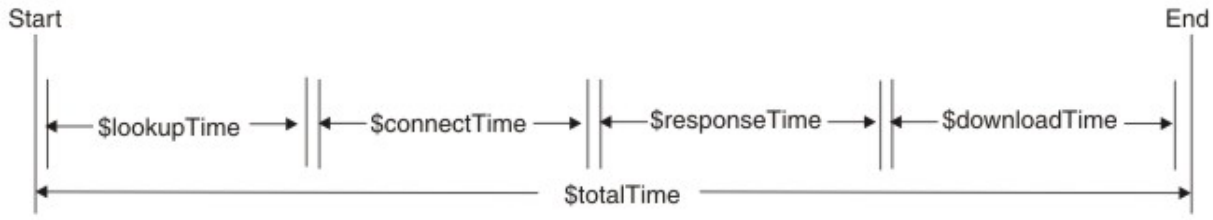
Tabla 36. Elementos comunes de supervisor	
Nombre de elemento	**Descripción de elemento**
$consecutiveFailures	Si $failureRetests es un valor distinto a cero y la prueba falla de acuerdo con la clasificación del nivel de servicio, este elemento se crea empezando con el valor 1. El valor aumenta hasta que la prueba deja de fallar, en cuyo punto $consecutiveFailures se establece en 0, o hasta el siguiente sondeo. Si, en este sondeo, se pasa el nivel de servicio o empieza a aumentar de nuevo, el elemento ya no se crea. Si el valor de este elemento excede el valor de $failureRetests, el valor de $consecutiveFailures se restablece en 1. **Nota:** El supervisor TRANSX no genera este elemento.
$datalogPath* (guid)	La vía de acceso del archivo del registro de datos utilizado por el supervisor. El atributo de espacio de trabajo utiliza los últimos 100 caracteres de la vía de acceso.
$description* (Description)	Contiene la descripción en texto proporcionada en el campo **Descripción** del elemento de perfil de supervisor.
$failureRetestInterval	El intervalo de sondeo utilizando durante la repetición de prueba. Esto solo es válido si $failureRetests es mayor que 0. Si el intervalo de repetición de prueba es mayor que el intervalo de sondeo normal, se establece en un valor igual al intervalo de sondeo normal. **Nota:** El supervisor TRANSX no genera este elemento.
$failureRetests	El número de errores de nivel de servicio que se debe superar antes de que se registre un suceso anómalo y se envíe a ObjectServer. **Nota:** El supervisor TRANSX no genera este elemento.
$host* (Host)	El nombre del host o del servidor. Se almacena en el archivo de configuración.
$hostName	Contiene el nombre de host del elemento $host (si $host es una dirección IP).
$hostIP	Contiene el IP de host del $host (si $host es un nombre DNS).
$identchecksum* (Identchecksum)	El identificador del elemento de perfil.
$lastServiceLevel* (LastServiceLevel)	El número del nivel de servicio del sondeo anterior. Este valor se borra si el perfil cambia.
$lastServiceLevelCounter	El valor serviceLevelCounter en el sondeo anterior. Este valor se restablece si cambia el perfil.
$monitorDNSdomain	El nombre de dominio de la máquina que ejecuta el supervisor, tal como lo utiliza el DNS.

Tabla 36. Elementos comunes de supervisor (continuación)	
Nombre de elemento	**Descripción de elemento**
$monitorHost* (MonitorLocation)	El nombre del host que ejecuta el supervisor.
$monitorNISdomain	El nombre de dominio del host que ejecuta el supervisor, tal como lo utiliza el NIS (Servicio de información de red).
$monitorDomain	Altera temporalmente los valores de $monitorDNSdomain y $monitorNISdomain.
$message* (ResultMessage)	Una cadena de texto que describe el resultado del sondeo. Por ejemplo, La conexión ha fallado, Correcto o Éxito.
(Node)	El nombre del sistema en el cual se está ejecutando Internet Service Monitoring. Este atributo se añadido por el agente de Internet Service Monitoring.
$pollInterval	El intervalo de sondeo especificado en cada supervisor.
$resultString* (ResultString)	Una serie de texto que indica la clasificación de nivel de servicio aplicada a los resultados del sondeo. Por ejemplo, TotalTime > 20.
$service* (Service)	Nombre del servicio que se está supervisando. Por ejemplo, FTP o HTTP.
$serviceLevel* (ServiceLevel)	El número de nivel de servicio del sondeo, tal como se define en la clasificación de nivel de servicio. 0 - Desconocido 1 - Correcto 2 - Marginal 3 - Anómalo
$serviceLevelCounter	El número de veces que el número de nivel de servicio se ha mantenido sin cambios.
(ServiceLevelString)	La cadena asociada al nivel de servicio devuelto (Desconocido, Correcto, Marginal o Anómalo).
$startTimePoll	La hora cuando se inició el sondeo.
$time	La hora de UNIX, en segundos, cuando se produjo el sondeo.
$timeStamp* (Timestamp)	La fecha y hora cuando se realizó la prueba. El formato de indicación de fecha y hora utiliza valores locales.
$transxName	Nombre de la transacción. Se genera mediante un supervisor, si el supervisor se utiliza en una transacción.
Detalles de perfil	

Tabla 36. Elementos comunes de supervisor (continuación)	
Nombre de elemento	**Descripción de elemento**
`$profile*` (`IsmProfile`)	Nombre del perfil de usuario.
Temporizaciones - si desea información sobre cómo se miden las temporizaciones, consulte "Cálculos de tiempo" en la página 327.	
`$timeout`	El número de segundos en los que debe responder el servidor. Se toma del archivo de configuración.
`$totalTime*` (`TotalTime`)	El tiempo total que se tarda en ejecutar una operación en segundos. Esto incluye todos los tiempos de búsqueda, conexión y descarga cuando es aplicable, y el tiempo de proceso temporal.

Cálculos de tiempo

Los supervisores intentan dividir el tiempo que se tarda en completar un sondeo en distintas etapas temporizadas. Por ejemplo, esto podría incluir el tiempo que se tarda en obtener la dirección IP de un host, o el tiempo que se tarda en conectarse correctamente a un host.



`$totalTime` siempre es ligeramente más largo que la suma de los otros tiempos, porque incluye la sobrecarga producida por las actividades del supervisor como, por ejemplo, el proceso de datos recibidos y la realización de llamadas del sistema. `$totalTime` se mide en segundos.

Mensajes de estado
Los supervisores devuelven los mensajes de estado generados después de cada prueba de servicio. Los mensajes de estado indican el resultado de las pruebas.

Los mensajes se suelen originar en el servicio supervisado o el entorno de red fuera del supervisor. Tabla 37 en la página 328 describe los mensajes de estados comunes devueltos por supervisores en el atributo `ResultMessage` al utilizar IBM Application Performance Management. Los mensajes de estado específicos de supervisor se describen en las secciones de cada supervisor.

Además de los mensajes proporcionados por los supervisores individuales, algunos supervisores como, por ejemplo, el supervisor HTTP, notifican mensajes para el sistema operativo subyacente. Por ejemplo, si la conexión TCP falla,Agente de Internet Service Monitoring utiliza la cadena definida por el sistema operativo como, por ejemplo, **`connection refused`**, **`timeout`**, **`network unreachable`** y otras cadenas.

Tabla 37. Mensajes de estado comunes

Mensaje	**Descripción**
CORRECTO	La solicitud del supervisor se ha realizado correctamente. Los supervisores pueden tener otros mensajes de estado que indican que un proceso se ha realizado correctamente. Consulte la sección *Mensaje de estado* para cada supervisor.
Se ha recibido una respuesta a la solicitud que no procede de este supervisor - se ignora	Se ha recibido una respuesta del servidor a un mensaje que no se ha originado en el supervisor designado.
Connection failed Ha fallado la conexión al servidor	El supervisor no ha podido conectarse al servidor. Consulte el archivo de registro si desea más información.
La conexión se ha cerrado inesperadamente	La conexión con el servidor se ha interrumpido.
La conexión ha agotado el tiempo de espera	La conexión se ha establecido correctamente, pero el servidor ha dejado de responder.
Conexión cerrada por un host externo	El host remoto ha cerrado la conexión antes de lo que esperaba el supervisor.
Tiempo de espera agotado mientras se espera leer/escribir	Se ha establecido una conexión de datos con el servidor de supervisión, pero ha dejado de responder.
Sin respuesta del servidor	La solicitud ha agotado el tiempo de espera.
Error de formato Error de servidor No existe ese host o dominio No implementado Solicitud rechazada Error desconocido	Error devuelto por el servidor supervisado.

Tabla 37. Mensajes de estado comunes (continuación)	
Mensaje	**Descripción**

`La red está desactivada`
`No se puede acceder a la red`
`Conexión descartada de la red al restablecer`
`El software ha provocado una terminación anormal de la conexión`
`Conexión restablecida por un igual`
`La conexión ha agotado el tiempo de espera`
`Conexión rechazada`
`El host está desactivado`
`Sin ruta al host`
`Conexión liberada por igual remoto`
	Hay un problema con la red.

Supervisor DHCP

El supervisor DHCP comprueba la disponibilidad y el tiempo de respuesta de los servidores DHCP.

Asigne las clasificaciones del nivel de servicio según el tiempo que necesite el servidor DHCP para responder a una solicitud del supervisor DHCP, usando el total, la búsqueda o el tiempo de respuesta.

Tabla 38. Archivos del supervisor DHCP	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_dhcp`
Archivo de propiedades	`$ISMHOME/etc/props/dhcp.props`
Archivo de reglas	`$ISMHOME/etc/rules/dhcp.rules`
Archivo de registro	`$ISMHOME/log/dhcp.log`

Directrices para la configuración del supervisor DHCP

El supervisor DHCP prueba los servicios DHCP actuando como un cliente DHCP limitado. Envía una solicitud DHCP INFORM al servidor DHCP de destino en la misma red usando UDP como protocolo de transporte mediante una conexión establecida, y espera un DHCP ACK correspondiente del servidor. El supervisor no solicita una dirección IP, ni afecta a la caducidad de las direcciones IP existentes.

Nota: Los servidores DHCP supervisados deben soportar las solicitudes DHCP INFORM y ser compatibles con RFC2131.

El supervisor DHCP debe ejecutarse como `root`, porque se vincula a un puerto inferior a 1024.

Limitación

El supervisor DHCP no puede utilizar ninguna interfaz de red configurada mediante un cliente DHCP. En lugar de ello, configure el supervisor para que utilice una interfaz de red cuya dirección IP no esté asignada dinámicamente.

Configuración de la prueba de servicio del supervisor DHCP

Tabla 39. Configuración del supervisor DHCP	
Campo	**Descripción**
server	Nombre de host del servidor DHCP. Por ejemplo, dhcp1.mycompany.com
localip	Interfaz de red de dirección IP que utiliza el supervisor para realizar la prueba. Por ejemplo, 192.168.n.n
description	Un campo de texto para proporcionar información descriptiva sobre el elemento. Por ejemplo, el supervisor DHCP
port	El número de puerto del servidor DHCP. El valor predeterminado es 67.
localport	Número de puerto que utiliza el supervisor para realizar la prueba. El valor predeterminado es 68.
timeout	Tiempo, en segundos, que se debe esperar a que responda el servidor. El valor predeterminado es 30.
retries	Número de veces que el supervisor debe volver a intentar la conexión al servidor DHCP antes de salir. El valor predeterminado es 0. Por ejemplo, 2.
poll	Tiempo, en segundos, entre cada sondeo del servidor utilizando el elemento de perfil actual. El valor predeterminado es 300.
failureretests	Número de veces que se debe realizar una nueva prueba antes de que se indique una anomalía. El valor predeterminado es 0.
retestinterval	Tiempo, en segundos, que se debe esperar entre cada nueva prueba en caso de anomalía. El valor predeterminado es 30.

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor DHCP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio DHCP.

Tabla 40. Elementos del supervisor DHCP	
Elemento	**Descripción**
`$clientIP*ClientIp`	Dirección IP del host en el que se está ejecutando el supervisor.
`$lookupTime*(LookupTime)`	Tiempo que se tarda en obtener la dirección IP del servidor de host.
`$responseTime*ResponseTime`	Tiempo entre el establecimiento de la conexión y la recepción del primer byte de datos.
`$retries`	Número máximo de reintentos, tal como se especifica durante la configuración del supervisor.

Tabla 40. Elementos del supervisor DHCP (continuación)	
Elemento	**Descripción**
`$router`	Dirección IP del direccionador devuelta por el servidor DHCP.

Mensajes de estado

El supervisor DHCP proporciona mensajes de estado en el atributo `ResultMessage` al utilizar IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

Tabla 41. Mensajes de estado del supervisor DHCP	
Mensaje	**Descripción**
`Received DHCPACK Received DHCPNAK` (Se ha recibido DHCPNAK)	Un servidor DHCP responde a la solicitud de informes de DHCP enviada por el supervisor.
`This monitor requires root privileges to run` (Este supervisor requiere privilegios root para ejecutarse)	Inicie la sesión como usuario root.
`Did not receive valid DHCP MESSAGE` (No se ha recibido un mensaje DHCP válido)	Respuesta no reconocida del servidor DHCP.
`Did not receive valid DHCP MESSAGE` (No se ha recibido un mensaje DHCP MESSAGE TYPE válido)	Respuesta no reconocida del servidor DHCP (se esperaba DHCPACK o DHCPNAK).
`Invalid transaction ID` (ID de transacción no válido) `Se ha recibido una respuesta a la solicitud que no procede de este supervisor - se ignora`	Se ha recibido una respuesta de un servidor DHCP a un mensaje que no se ha originado en este supervisor.
`Unexpected op-code returned` (Se ha devuelto un código de operación inesperado)	Se ha recibido un mensaje inesperado en este puerto.
`Connection failed` (Error de conexión)	El nombre de servidor especificado no es válido.
`Failed to send request to DHCP server` (No se ha podido enviar la solicitud al servidor DHCP)	El sistema operativo no puede identificar específicamente por qué la solicitud no se ha podido enviar al servidor, por lo que devuelve este mensaje de estado que indica que hay problema con la red.
`No Response from server` (No hay respuesta del servidor)	El servidor DHCP no responde.

Supervisor DNS

El supervisor DNS utiliza el servicio DNS (Sistema de nombres de dominio) para encontrar información sobre uno o varios hosts.

El supervisor DNS utiliza la dirección IP del host para buscar el nombre de host, o el nombre de buscar para buscar la dirección IP. El supervisor mide el rendimiento del servicio registrando el resultado de los tiempos de búsqueda y de respuesta. El supervisor también registra detalles sobre cada consulta enviada al servidor.

Tabla 42. Resumen de archivos de supervisor DNS	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_dns`
Archivo de propiedades	`$ISMHOME/etc/props/dns.props`
Archivo de reglas	`$ISMHOME/etc/rules/dns.rules`
Archivo de registro	`$ISMHOME/log/dns.log`

Directrices para configurar el supervisor DNS

El supervisor DNS se puede configurar para buscar la dirección IP o el nombre de host del host de destino. En función del tipo de búsqueda, el supervisor se comunica con el servidor DNS de una forma diferente.

Búsqueda de direcciones IP

Al realizar una prueba de búsqueda de direcciones IP, se proporciona al supervisor un nombre de host, que utiliza para localizar una dirección IP.

El supervisor prueba el DNS del modo siguiente:

1. El supervisor consulta el servidor DNS utilizando el nombre de host completo de un HostA (`hosta.dev.net`) para solicitar su dirección IP.

   Si el servidor DNS puede localizar la dirección IP del host, la devuelve al supervisor. Si el servidor DNS no puede localizar la dirección IP del host, devuelve un mensaje que contiene detalles de la búsqueda fallida al supervisor.

   Si la solicitud ha agotado el tiempo de espera, el supervisor lo volverá a intentar (si se han configurado reintentos). Si no hay reintentos, el supervisor creará un suceso anómalo.

   Si el nombre de host especificado en la configuración es un nombre de dominio como, por ejemplo, `mycompany.com`, en lugar de un nombre de host completo, como `hostx.mycompany.com`, el supervisor recupera información sobre todo el dominio. Esta información se almacena en dos elementos adicionales: `$domainNameServer` y `$domainNameAddr`.
2. Si el mensaje devuelto al supervisor contiene un nombre canónico, el supervisor concluye que el nombre proporcionado en el archivo de configuración debe haber sido un alias. El supervisor envía el nombre canónico al servidor DNS para solicitar la dirección IP del host.

   Si el servidor DNS localiza la dirección IP del host utilizando su nombre canónico, la devuelve al supervisor. Si el servidor DNS no puede localizar la dirección IP del host, devuelve un mensaje que contiene detalles de la búsqueda fallida al supervisor.
3. Si los primeros dos intentos para consultar el servidor DNS fallan, el supervisor envía la dirección IP del servidor DNS (`192.168.n.n`) al servidor DNS y solicita su nombre de host completo.

   Si el servidor DNS puede localizar su propio nombre de host completo, lo devuelve al supervisor. Si el servidor DNS no puede localizar su nombre de host completo, devuelve un mensaje que contiene los detalles de la búsqueda fallida. La solicitud para el nombre de host completo del servidor (una solicitud de búsqueda de DNS inversa) no está soportada en todos los tipos de servidores DNS. Si el servidor DNS de destino no admite las búsquedas inversas, puede impedir que el servidor DNS envíe esta solicitud estableciendo la propiedad `LookupServerName` en `0`.

Búsqueda recursiva

Las búsquedas no recursivas presentan una imagen más precisa sobre el funcionamiento del servidor DNS, mientras que las búsquedas recursivas proporcionan una mejor indicación del rendimiento de DNS que obtienen las aplicaciones de Internet (y, por lo tanto, los usuarios). El supervisor DNS admite ambas búsquedas, recursivas y no recursivas.

Normalmente, así es como funcionan las aplicaciones de Internet que realizan consultas DNS. Por ejemplo, un navegador web especifica siempre búsquedas recursivas cuando intenta resolver la parte de host de un URL.

Si un servidor DNS no puede responder a una consulta porque no contiene una entrada para el host en su base de datos, puede consultar de forma recursiva servidores DNS más altos en la jerarquía.

Tipos de consulta DNS

El supervisor DNS admite un rango de tipos de consulta DNS. Utilice el código de consulta al especificar el tipo de consulta DNS.

Tabla 43. Tipos de consulta DNS

Código de consulta	Tipo de consulta
A	Dirección de host
NS	Servidor de nombres autorizado
MD	Destino de correo
MF	Reenviador de correo
CNAME	Nombre canónico para un alias
SOA	Inicio de una zona de autorización
MB	Nombre de dominio de buzón
MG	Miembro de grupo de correo
MR	Nombre de dominio de redenominación de correo
NULL	RR nulo
WKS	Descripción de servicio conocido
PTR	Puntero de nombre de dominio
HINFO	Información de host
MINFO	Información de lista de buzón o correo
MX	Intercambio de correo
TXT	Cadenas de texto
AXFR	Transferencia de una zona entera
MAILB	Registros relacionados con el buzón
MAILA	RR de agente de correo
ANY	Todos los registros

Configuración de pruebas de servicio de supervisor DNS

Utilice los parámetros de configuración de supervisor DNS para definir pruebas de servicio DNS.

Tabla 44. Tabla 3. Configuración de supervisor DNS

Campo	Descripción
server	La dirección IP del servidor DNS primario. El ejemplo es 192.168.n.n
host	El nombre de host del host de destino. El ejemplo es www.myconpany.com

Tabla 44. Tabla 3. Configuración de supervisor DNS (continuación)	
Campo	**Descripción**
description	Un campo de texto para proporcionar información descriptiva sobre el elemento. El ejemplo es el supervisor DNS.
recursivelookups	Habilita o inhabilita búsquedas recursivas. • `recurse` (utilizar `true` en ismbatch). • `norecurse` (utilizar `false` en ismbatch). Valor predeterminado: `recurse`.
port	El puerto del servidor DNS en el que escucha el supervisor y el valor predeterminado es 53.
localip	Especifica la dirección IP de la interfaz de red en la máquina de host a la que se enlaza el supervisor cuando realizar la prueba. Si la propiedad `IpAddress` del supervisor está establecida, altera temporalmente el valor de este campo.
querytype	El tipo de consulta DNS utilizado en la prueba. Si desea una lista de tipos de consulta soportados, consulte Tabla 43 en la página 333.
timeout	El tiempo, en segundos, de espera para que responda el servidor. Valor predeterminado: `10`.
retries	El número de veces que el supervisor debe reintentar contactar con el servidor DNS antes de salir.
poll	El tiempo, en segundos, entre cada sondeo. Valor predeterminado: `300`.
failureretests	El número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: `0`.
retestinterval	El tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: `10`.

Elementos de supervisión

Además de los resultados de prueba comunes para todos los elementos, el supervisor DNS genera un conjunto de resultados de prueba que contienen datos específicos de las pruebas de servicio DNS.

Tabla 45. Tabla 4.Elementos de supervisor DNS	
Elemento	**Descripción**
`$authoritative`	Este elemento solo se crea si la información recuperada procedía de un servidor DNS autorizado. Si el servidor DNS no estaba autorizado, este elemento no se crea.
`$domainEmailAddr`	La dirección de contacto del dominio de destino.
`$domainNameServer`	El nombre del servidor DNS para el dominio de destino.

Tabla 45. Tabla 4.Elementos de supervisor DNS (continuación)	
Elemento	**Descripción**
$fromAliasTime	El tiempo transcurrido entre el envío de una solicitud para un nombre canónico, recibida de una consulta anterior, y la recepción de una dirección IP.
$localIP	La dirección IP local configurada para ser utilizada por el supervisor. Este valor puede estar en blanco en una máquina con solo una interfaz.
$lookup*(HostLookup)	El nombre de host o la dirección IP del host de destino que el supervisor está intentando localizar.
$lookupCName	El nombre de host oficial del host de destino. Este elemento solo se crea si el nombre de host oficial es diferente del nombre de host en $lookupName.
$lookupIP*(HostIp)	La dirección IP del host de destino.
$lookupName*(Host)	El nombre de host completo del host de destino.
$mxRecords	El número de registros MX encontrados.
$port	Puerto en que se supervisa el servicio.
$queryType	El tipo de consulta DNS utilizada en la prueba. Si desea una lista de tipos de consulta soportados, consulte Tabla 43 en la página 333.
$responseTime*(ResponseTime)	El tiempo transcurrido desde que el supervisor emite una solicitud al servidor DNS y la recepción de una respuesta de este.
$retries	El número máximo de reintentos, como se especifica en el elemento de perfil.
$serverIP	La dirección IP del servidor DNS.
$serverName	El nombre de host del servidor DNS.
$serverTime	El tiempo que tiene el servidor para resolver su propio nombre.

Manejo de registros MX

Se crean dos elementos para cada registro MX encontrado por el supervisor DNS: $mxHostn y $mxPreferencen.

$mxHostn almacena el nombre de host de un registro MX. $mxPreferencen contiene la ponderación de preferencia del host. n aumenta para cada par de registros para diferenciarlos. El supervisor almacena el número total de registros MX para un host concreto en el elemento $mxRecords. Los pares de registros se clasifican en orden descendente de preferencia MX.

Mensaje de estado

El supervisor DNS proporciona mensajes de estado en el atributo ResultMessage cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

Tabla 46. Tabla 5.Mensajes de estado de supervisor DNS	
Mensaje	**Descripción**
Información de dominio recibida	La solicitud de un nombre de dominio se ha realizado correctamente.
Success	La solicitud se ha realizado correctamente.

Tabla 46. Tabla 5.Mensajes de estado de supervisor DNS (continuación)	
Mensaje	**Descripción**
`Respuesta no válida`	Respuesta no reconocida del servidor DNS.
`Conexión fallida`	El nombre de servidor especificado no es válido.
`Sin respuesta del servidor`	La solicitud ha agotado el tiempo de espera.
`No se ha podido enviar la solicitud de DNS`	Hay un problema con la red.
`No existe dicho dominio (sin recurrencia)`	El nombre de dominio es incorrecto.

Propiedades

Las propiedades específicas del supervisor DNS se describen en la tabla siguiente.

Tabla 47. Propiedades de supervisor DNS		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
`AcceptCNAME`	`0`|`1`	Si está habilitado, el supervisor DNS acepta el nombre canónico en la respuesta DNS y no realiza más búsquedas.
`DNSQueryType`	serie	El tipo de consulta DNS utilizado en pruebas. Consulte Tabla 43 en la página 333 si desea una lista de tipos de consulta soportados. Valor predeterminado: `ANY`.
`LookupServerName`	`0`|`1`	Habilita la búsqueda de DNS inversa en la dirección IP del servidor DNS. `0` - inhabilitado `1` - habilitado

Supervisor FTP

El supervisor FTP prueba los servicios FTP cargando archivos a los servidores FTP o descargándolos de ellos. Supervisa el rendimiento del servicio registrando el tiempo de respuesta y la velocidad de transferencia de datos, y supervisa el espacio en disco y la integridad de los archivos.

Tabla 48. Resumen del supervisor FTP	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_ftp`
Archivo de propiedades	`$ISHOME/etc/props/ftp.props`
Archivo de reglas	`$ISHOME/etc/rules/ftp.rules`
Archivo de registro	`$ISHOME/log/ftp.log`

Directrices para configurar el supervisor FTP

El supervisor FTP prueba la disponibilidad de un servidor FTP cargando un archivo al servidor mediante un mandato FTP STOR, o descargando un archivo del servidor con un mandato FTP RETR.

Configuración de pruebas de servicio de supervisor FTP

Los parámetros de configuración para el supervisor FTP se describen en la tabla siguiente.

Tabla 49. Configuración del supervisor FTP

Campo	Descripción
server	Dirección IP del servidor FTP de destino o la máquina desde la que se desea transferir por FTP. Por ejemplo, `ftp.mycompany.com`
localfile	Para las operaciones GET de FTP, este campo especifica el nombre y la vía de acceso donde se descarga el archivo. Para las operaciones PUT de FTP, este campo especifica el nombre y la vía de acceso del archivo que se carga en el servidor FTP. El valor predeterminado es FULL PATHNAME. Por ejemplo, `$ISMHOME/etc/ism/downloads/ftp-test.tar.Z`
remotefile	Para las operaciones GET de FTP, este campo especifica el nombre y la vía de acceso del archivo que se descarga del servidor. Para las operaciones PUT de FTP, este campo especifica el nombre y la vía de acceso donde se carga el archivo al servidor FTP. El valor predeterminado es FULL PATHNAME. Por ejemplo, `/sales/prodlist.tar.Z`
description	Campo de texto para proporcionar información descriptiva sobre el elemento.
port	El puerto predeterminado que utiliza el servidor FTP. Valor predeterminado: 21
username	Nombre de usuario que se utiliza para iniciar la sesión en el servidor FTP de destino.
password	Contraseña que se utiliza para iniciar la sesión en el servidor FTP de destino. Deje este espacio en blanco si la cuenta de FTP no requiere una contraseña.
command	Mandato FTP que debe utilizar el supervisor: • GET o RECV: descarga un archivo desde el servidor FTP de destino • SEND o PUT: carga un archivo en el servidor FTP de destino Valor predeterminado: GET.
conntype	Especifica el tipo de conexión que debe establecer el supervisor con el servidor al intentar transferir el archivo: • `Activo` • `Pasivo` Valor predeterminado: `Activo`.

Tabla 49. Configuración del supervisor FTP (continuación)	
Campo	**Descripción**
timeout	El tiempo, en segundos, de espera para que responda el servidor. Valor predeterminado: `30`.
poll	El tiempo, en segundos, entre cada sondeo. Valor predeterminado: `300`
failureretests	El número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: `0`.
retestinterval	El tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: `10`.

Coincidencia de expresiones regulares

Puede realizar una búsqueda de expresiones regulares en la información que se está descargando especificando hasta 50 expresiones regulares diferentes. El supervisor FTP intenta hacer coincidir el contenido recuperado con cada una de las expresiones regulares.

Si se encuentra una coincidencia para cada una expresión regular especificada, las líneas coincidentes (o todas las que quepan en el almacenamiento intermedio del supervisor) se devuelven en el elemento `$regexpMatchn` correspondiente. Si la expresión regular coincide más de una vez en la información descargada, sólo se devuelve la primera coincidencia. El estado de cada prueba de expresión regular se indica con los elementos `$regexpStatusn`. Puede utilizar las coincidencias de expresiones regulares y su información de estado como criterios para las clasificaciones del nivel de servicios.

Las expresiones regulares establecen la coincidencia de cadenas con respecto al contenido descargado durante las pruebas de servicios. Dichas expresiones pueden contener uno o varios operadores de expresiones regulares, que determinan el contenido con el que debe coincidir la expresión.

Nota: La sintaxis de expresiones regulares sólo se puede utilizar para coincidir con cadenas en líneas individuales. Internet Service Monitoring no puede hacer coincidir series que incluyan líneas nuevas o retornos de carro. Utilice varias expresiones regulares para la coincidencia de las series que abarquen varias líneas. También puede utilizar reglas de SLC para que se emitan alarmas en función del resultado de varias expresiones regulares.

Tabla 50. Operadores de expresiones regulares	
Carácter	**Descripción**
.	Establece una coincidencia con cualquier carácter individual. Por ejemplo, la expresión regular `r.t` coincide con las series `rat`, `rut`, `r t`, pero no `root`.
$	Establece la coincidencia del final de una línea. Por ejemplo, la expresión regular `perro$` coincide con el final de la cadena `es un perro`, pero no con la cadena `Hay muchos perros`.

Tabla 50. Operadores de expresiones regulares (continuación)	
Carácter	**Descripción**
^	Establece la coincidencia del principio de una línea. Por ejemplo, la expresión regular ^En el coincide con el inicio de la cadena En el curso de los acontecimientos pero no con Lo que sucede en el curso de los acontecimientos.
*	Establece la coincidencia de cero o varias apariciones del carácter inmediatamente anterior. Por ejemplo, la expresión regular .* coincide con cualquier número de caracteres.
\	Trata el carácter posterior como un carácter normal. Por ejemplo, \$ coincide con el carácter del símbolo del dólar ($) y no con el final de una línea. Del mismo modo, la expresión \. coincide con el carácter de punto y no con cualquier carácter individual.
[]	Establece la coincidencia de cualquier carácter contenido entre los corchetes. Por ejemplo, la expresión regular r[aou]t coincide con rat, rot y rut, pero no con rit. Puede especificar rangos de caracteres mediante un guion. Por ejemplo, la expresión regular [0-9] coincide con cualquier número. También puede especificar varios rangos. Por ejemplo, la expresión regular [A-Za-z] coincide con cualquier letra en mayúsculas o minúsculas.
|	Coincide con frases que contienen una de las condiciones especificadas. Por ejemplo él|ella coincide con la línea es de él y la línea es de ella, pero no con la línea es de ellos.

Nota: Si prefiere las series de datos de salida con llaves {} o comillas dobles "", tendrá que añadir un carácter de escape barra inclinada invertida \ antes de cada llave y comillas dobles en la expresión regular.

Por ejemplo, si la serie de datos es {"templates":true,"mongodb":true,"ldap":true,"ucd":true,"github":true}, la expresión regular debe aparecer como \{\"templates\":true,\"mongodb\":true,\"ldap\":true,\"ucd\":true,\"github\":true\}

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor FTP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio FTP.

Tabla 51. Elementos del supervisor FTP	
Elemento	**Descripción**
$bytesPerSec*(BytesPerSec)	Número promedio de bytes transferidos cada segundo.
$bytesTransfered* (BytesTransferred)	El número de bytes cargados o descargados.

Tabla 51. Elementos del supervisor FTP (continuación)	
Elemento	**Descripción**
`$checksum`	El elemento Checksum normalmente no proporciona valores significativos para para las clasificaciones del nivel de servicio porque los valores de la suma de comprobación no aparecen cuando el elemento de perfil se crea (el supervisor calcula los valores de la suma de comprobación mientras las pruebas están en progreso). Los elementos de supervisor $checksum y $previousChecksum están pensados para el enriquecimiento de alertas mediante el archivo de reglas del supervisor.
`$command*(FtpCommand)`	Mandato FTP que emite el supervisor.
`$connectionType*(FtpConnection)`	Tipo de conexión de datos utilizado. Puede ser `ACTIVE` o `PASSIVE`.
`$connectTime*(ConnectTime)`	Tiempo que se tarda en conectar con el servidor FTP.
`$downloadTime`	El tiempo que se tarda en descargar el archivo.
`$localFile*(FtpLocalFile)`	Nombre de vía de acceso completa del archivo almacenado en el host local. Este elemento se toma del archivo de configuración.
`$lookupTime*(LookupTime)`	Tiempo que se tarda en buscar la dirección IP del servidor FTP.
`$previousChecksum`	El elemento PreviousChecksum normalmente no proporciona valores significativos para las clasificaciones del nivel de servicio porque los valores de la suma de comprobación no aparecen cuando el elemento de perfil se crea (el supervisor calcula los valores de la suma de comprobación mientras las pruebas están en progreso). Los elementos de supervisor $previousChecksum y $checksum están pensados para el enriquecimiento de alertas mediante el archivo de reglas del supervisor.
`$regexp`*n*	La expresión regular.
`$regexpMatch`*n*	El contenido de la línea que coincide con la expresión regular.
`$regexpStatus`*n*	El estado de la coincidencia de la expresión regular: `NONE`: no se configura ninguna comprobación de expresión regular. `MATCHED`: se ha encontrado una coincidencia para la expresión regular. `FAILED`: no se ha encontrado ninguna coincidencia para la expresión regular
`$remoteFile*(FtpRemoteFile)`	Nombre de vía de acceso completa del archivo almacenado en el host remoto (el servidor FTP). Este elemento se toma del archivo de configuración.
`$responseTime*(ResponseTime)`	El tiempo necesario, después de la creación de una conexión, hasta que se reciba el primer byte del archivo de destino.
`$status`	El código de estado devuelto por el servidor FTP.
`$transferTime*(TransferTime)`	Establece el valor en `$uploadTime` o `$downloadTime`.
`$uploadTime`	El tiempo que se tarda en cargar el archivo.

Tabla 51. Elementos del supervisor FTP (continuación)	
Elemento	**Descripción**
`$username`	El nombre de usuario (nombre de cuenta) utilizado por el supervisor para iniciar la sesión en el host de destino. Este elemento se toma del archivo de configuración si `$message` contiene OK.

Mensajes de estado

El supervisor FTP proporciona mensajes de estado en el atributo `ResultMessage` cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

Tabla 52. Mensajes de estado del supervisor FTP	
Mensaje	**Descripción**
`Aceptar`	La solicitud FTP se ha realizado correctamente.
`Unable to open local file for reading/writing` (No se ha podido abrir el archivo local para la lectura/escritura)	Consulte el archivo de registro del supervisor FTP para ver más información.
`Unable to read from/write to local file` (No se puede leer de/escribir en el archivo local)	
`Unable to read from data connection` (No se puede leer de la conexión de datos)	Se ha establecido una conexión de datos con el servidor FTP, pero se ha producido un problema.
`Unable to upload to ftp server` (No se puede cargar en el servidor FTP)	
`Timed out waiting to read/write` (Tiempo de espera superado al esperar lectura/escritura)	
`Connection closed by foreign host` (Conexión cerrada por host foráneo)	La conexión con el servidor FTP se ha interrumpido.
`Connection closed unexpectedly` (Conexión cerrada de forma inesperada)	
`Connection failed` (Error de conexión)	El supervisor no ha podido conectarse con el servidor FTP. Consulte el archivo de registro del supervisor FTP para ver más información.

Supervisor HTTP

El supervisor HTTP comprueba la disponibilidad y el tiempo de respuesta de los servidores web.

Puede supervisar páginas web individuales, incluidas las que utilizan CGI, que normalmente requerirían que el usuario especificara datos en campos. También puede supervisar el tiempo de descarga para elementos como, por ejemplo, imágenes en una página web.

Tabla 53. Resumen de archivos de supervisor HTTP	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_http`
Archivo de propiedades	`$ISHOME/etc/props/http.props`
Archivo de reglas	`$ISHOME/etc/rules/http.rules`

Tabla 53. Resumen de archivos de supervisor HTTP (continuación)	
Archivos de supervisor	**Nombre o ubicación**
Archivo de registro	`$ISHOME/log/http.log`

Directrices para configurar el supervisor HTTP

Los supervisores HTTP y HTTPS comprueban la disponibilidad y el tiempo de respuesta de servidores web. Utilice el supervisor HTTP en las situaciones siguientes:

- El sitio web de destino es estático.

  Para sitios web dinámicos, utilice el supervisor TRANSX.
- Se presta servicio al sitio web de destino mediante el protocolo HTTP.

  Para sitios web que entregan contenido a través del protocolo HTTPS, seleccione el supervisor HTTPS.
- Para realizar la supervisión entre varias plataformas.
- Cuando la velocidad es un factor determinante (el supervisor HTTP proporciona alto rendimiento).

Tipos de solicitud HTTP

El supervisor HTTP emula un navegador web que admite el protocolo HTTP/1.0. Para probar el servidor web, el supervisor le envía una solicitud para una página web utilizando cualquiera de los tipos de solicitud HTTP siguientes:

- `HEAD`

  El mandato `HEAD` intenta acceder a una página web y devolver la cabecera HTTP. La emisión de un mandato `HEAD` es una manera rápida de comprobar que se puede acceder a una página web.
- `GET`

  El mandato `GET` intenta acceder a la página web y devolver la página entera, incluida la cabecera HTTP. No intenta devolver archivos asociados a la página como, por ejemplo, imágenes.
- `GETALL`

  El mandato `GETALL` intenta acceder a la página web y devolver toda la página, incluyendo la cabecera HTTP, el fondo, imágenes, applets, marcos, archivos de hoja de estilo en cascada (CSS) y scripts. Al igual que los mandatos `HEAD` y `GET`, este mandato también comprueba que se puede acceder a una página web, pero puesto que el mandato `GETALL` devuelve toda la página y todos sus archivos asociados, puede ofrecer una indicación más realista del tiempo que se tarda en acceder a la página. El supervisor también utiliza varias hebras durante un mandato `GETALL` para que coincida con más precisión el comportamiento de los navegadores web.
- `POST`

  El mandato `POST` intenta acceder a una página web que contiene un formulario HTTP y completar los campos de dicho formulario. Añada texto de cuerpo para la solicitud POST al separador **Cuerpo** en la configuración de Agente de Internet Service Monitoring, o utilice el grupo `@Body` en la configuración de Agente de Internet Service Monitoring o ismbatch. De forma alternativa, puede utilizar los parámetros FORM. No puede utilizar a la vez el texto de cuerpo y los parámetros FORM en la solicitud POST.

Utilización de un servidor proxy

Puede probar la disponibilidad de páginas web a través de un servidor proxy. Al configurar el supervisor para utilizar un proxy, envía solicitudes HTTP a través del proxy. Si es necesario, puede omitir la memoria caché de proxy. Configure los parámetros para el servidor proxy en el separador **Detalles de proxy**. El supervisor HTTP admite el acceso autenticado a servidores proxy. Esta autenticación es independiente de cualquier autenticación que necesite la página web de destino.

Elementos de servidor proxy

En versiones anteriores, cuando ha configurado un elemento de perfil para que utilice un servidor proxy, de forma predeterminada el supervisor HTTP ha insertado el nombre del servidor proxy y el puerto en los elementos `$server` y `$port`. Para conservar el valor del nombre y el puerto del servidor de destino pensado en versiones anteriores, establezca la propiedad `generateProxyTokens` en `1` o inicie el supervisor con el parámetro de línea de mandatos `-generateproxytokens`.

Además de conservar los valores de los elementos `$server` y `$port` cuando está establecida esta propiedad o este parámetro de línea de mandatos, el supervisor genera los elementos `$proxyServer`, `$proxyPort`, `$proxyAuthType`, `$proxyUsername` y `$proxyCache`.

Autenticación

Si la página web que desea supervisar, o el servidor proxy que desea probar, requiere autenticación, especifique credenciales para acceder a la página en los campos de parámetro `authenticationtype`, `username` y `password` en la pestaña Avanzado o Detalles de proxy.

Para inhabilitar la autenticación, configure `authenticationtype` en `NONE`.

Para seleccionar la autenticación básica:

1. Establezca `authenticationtype` en `BASIC`.
2. Establezca `username` y `password` en los valores necesarios para la página web o el servidor proxy.

Para seleccionar NTLM:

1. Establezca `authenticationtype` en `NTLMv1` o `NTLMv2`.
2. Establezca `username` y `password` en los valores necesarios para la página web o el servidor proxy.

Nota:

El supervisor limita la longitud de las solicitudes HTTP a 4096 caracteres. Si la longitud de los datos de formulario adicionales da como resultado una longitud de solicitud que excede este límite, el supervisor no incluye los datos de formulario adicionales en la solicitud.

Configuración de la prueba de servicio de supervisor HTTP

Utilice los parámetros de configuración del supervisor HTTP para definir pruebas de servicio HTTP.

Tabla 54. Configuración del supervisor HTTP

Campo	Descripción
server	El nombre de host del servidor que se va a supervisar. El ejemplo es `www.mycompany.com`
page	El URL de la página que se va a supervisar. El ejemplo es `index.html`
description	Un campo de texto para proporcionar información descriptiva sobre el elemento. El ejemplo es `supervisión a través de un servidor proxy`
port	El puerto en el servidor HTTP para utilizar. Valor predeterminado: `80`
localip	Especifica la dirección IP de la interfaz de red que utiliza el supervisor para la prueba. Si este campo está en blanco, el supervisor utiliza la interfaz especificada por la propiedad `IpAddress`.

Tabla 54. Configuración del supervisor HTTP (continuación)	
Campo	**Descripción**
version	La versión de protocolo HTTP que se va a utilizar: • `1.0` • `1.1` Valor predeterminado: `1.0`
command	El tipo de solicitud HTTP. • `HEAD` • `GET` • `GETALL` • `POST` Valor predeterminado: `GET`
formname	Cuando se utiliza en una transacción, el supervisor HTTP explora el formulario especificado para valores predeterminados. Los valores encontrados se llenan automáticamente en el siguiente paso HTTP en la transacción.
authenticationtype	Especifica el mecanismo de respuesta de verificación de identidad para autenticar usuarios de red: • `NONE`: sin autenticación • `BASIC` • `NTLMv1`: Autenticación de respuesta de verificación de identidad de Windows NTLM versión 1 • `NTLMv2`: Windows NTLM versión 2 Valor predeterminado: `NONE`
username	El nombre de usuario (nombre de cuenta) que el supervisor debe utilizar para iniciar sesión en el servidor.
password	La contraseña correspondiente al nombre de usuario que el supervisor debe utilizar para iniciar sesión en el servidor.
timeout	El tiempo, en segundos, de espera a que responda el servidor. Valor predeterminado: `30`
poll	El tiempo, en segundos, entre cada sondeo. Valor predeterminado: `300` .
failureretests	El número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: `0`
retestinterval	El tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: `10`
verifycertificate	De forma predeterminada está inhabilitado.

Tabla 54. Configuración del supervisor HTTP (continuación)	
Campo	**Descripción**
Detalles de proxy	
server	El nombre de host del servidor proxy.
port	El puerto en el servidor proxy para utilizar. Valor predeterminado: `8080`
authenticationtype	El tipo de autenticación de servidor para el servidor proxy. Para obtener más información, consulte el elemento `authenticationtype` anterior. Valor predeterminado: `NONE`
username	Utilizado por el supervisor junto con la contraseña para iniciar sesión en el servidor proxy.
password	Utilizado por el supervisor junto con el nombre de usuario para iniciar sesión en el servidor proxy y la etiqueta es la contraseña.
useproxy	Configura el supervisor para realizar la solicitud utilizando un servidor proxy. • `proxy` (utilizar `true` en ismbatch) • `noproxy` (utilizar `false` en ismbatch) Valor predeterminado: `noproxy`
hostnamelookuppreference	Determina qué versión de IP, IPv6 o IPv4, se aplica al nombre de host proporcionado. Las opciones son las siguientes: • `default` define el supervisor para utilizar valores de propiedades de nivel de supervisor. Es el valor predeterminado. • 4Then6 selecciona IPv4 y, después, IPv6. Utiliza direcciones IPv4 si están disponibles. Si no se encuentra ninguna dirección IPv4, se utilizan direcciones IPv6. • 6Then4 seleccione IPv6 y, después, IPv4. Utiliza direcciones IPv6 si están disponibles. Si no se ha encontrado ninguna dirección IPv6, se utilizan direcciones IPv4. • `4Only` solo selecciona IPv4. Solo utiliza direcciones IPv4. Si no hay ninguna dirección IPv4, el sondeo devuelve un error. • `6Only` solo selecciona IPv6. Solo utiliza direcciones IPv6. Si no hay ninguna dirección IPv6, el sondeo devuelve un error. • `6or4` selecciona IPv4 o bien IPv6. Utiliza la primera dirección devuelta desde el nombre de host.
nocache	De forma predeterminada, está establecido en memoria caché.

Expresión regular

Puede realizar una búsqueda de expresiones regulares en la información que se está descargando especificando hasta 50 expresiones regulares diferentes. El supervisor HTTP intenta coincidir con el contenido recuperado en cada una de las expresiones regulares. Si se encuentra una coincidencia para cada una expresión regular especificada, las líneas coincidentes (o todas las que quepan en el almacenamiento intermedio del supervisor) se devuelven en el elemento `$regexpMatchn` correspondiente. Si la expresión regular coincide más de una vez en la información descargada, solo se devuelve la primera coincidencia. El estado de cada prueba de expresión regular se indica con los elementos `$regexpStatusn`. Puede utilizar las coincidencias de expresiones regulares y su

información de estado como criterios para las clasificaciones del nivel de servicios. Consulte Tabla 50 en la página 338 si desea información sobre la sintaxis de expresión regular.

Parámetro de cabecera y formulario

El supervisor HTTP puede enviar datos adicionales en los campos de cabecera y el cuerpo del mensaje de solicitudes HTTP.

Configure los parámetros para estos datos adicionales en el separador Parámetros. Los parámetros son Nombre, Valor y Tipo y funcionan del modo siguiente:

- Los pares Nombre-Valor del tipo HEAD especifican campos de cabeceras adicionales como, por ejemplo, `User-Agent` y `Referer`, incluidos en todas las solicitudes HTTP enviadas por el supervisor. Los campos de cabecera pueden especificarse para cualquier tipo de método HTTP (`GET`, `GETALL`, `HEAD` o `POST`).

  Para ITCAM for Transactions V7.4.0.1 y posteriores, el parámetro de cabecera del agente de usuario predeterminado, `Mozilla/5.0 (ISM-MONITOR)` se añade para cada elemento HTTP o HTTPS nuevo. La cabecera de agente-usuario predeterminada es la que pueden utilizar los supervisores HTTP y HTTPS para sitios web que conmutan el contenido basándose en el cliente de navegador.
- Los pares Nombre-Valor del tipo FORM especifican datos adicionales incluidos en el cuerpo del mensaje de las solicitudes HTTP `POST` enviadas por el supervisor. Si la página de destino contiene un formulario que coincide con el nombre especificado en el campo nombre_formulario, el supervisor trata los pares nombre-valor en el formulario como si se hubieran configurado en el elemento de perfil.

Nota:

El supervisor limita la longitud de las solicitudes HTTP a 4096 caracteres. Si la longitud de los datos de formulario adicionales da como resultado una longitud de solicitud que excede este límite, el supervisor no incluye los datos de formulario adicionales en la solicitud.

Elementos de supervisor

Además de los resultados de pruebas comunes a todos los elementos, el supervisor HTTP genera un conjunto de resultados de pruebas que contienen datos específicos a pruebas de servicio HTTP. Los elementos indicados por un asterisco (*) están disponibles como atributo. Los nombres de los atributos se muestran entre corchetes. La ausencia de un asterisco indica que no hay ningún atributo equivalente. Los atributos que se muestran entre corchetes, pero sin un elemento indican que solo están disponibles como atributo, no hay ningún elemento equivalente.

Tabla 55. Elementos de supervisor HTTP

Elemento	Descripción
`$bytesPerSec*(BytesPerSec)`	Número promedio de bytes transferidos cada segundo.
`$bytesTransfered*(BytesTransferred)`	El número de bytes cargados o descargados.
`$checksum`	El elemento Checksum normalmente no proporciona valores significativos para las clasificaciones del nivel de servicio porque los valores de la suma de comprobación no se conocen cuando se crea el elemento de perfil (el supervisor calcula los valores de la suma de comprobación mientras las pruebas están en curso). Los elementos de supervisor $checksum y $previousChecksum están diseñados para la mejora de la alerta mediante el archivo de reglas del supervisor.
`$command`	El mandato HTTP emitido por el supervisor. Por ejemplo, `HEAD`, `GET`, `GETALL` o `POST`.

Tabla 55. Elementos de supervisor HTTP (continuación)	
Elemento	**Descripción**
$connectTime*(ConnectTime)	El tiempo que se tarda en conectarse al servidor.
$downloadTime*(DownloadTime)	El tiempo que se tarda en descargar el archivo.
(Elements)	El número de elementos de página recibidos.
$formname	El nombre del formulario utilizado en una acción POST.
$lastStatus*(PageStatus)	Si un elemento de perfil recupera varias páginas, este elemento contiene la cadena del resultado de la última página recuperada. Este valor es el mismo que el valor de $urlResult*n* donde *n* es igual al valor de $pageCount.
$lastModified	El valor del campo de cabecera HTTP Last-Modified de la primera página recuperada.
$page*(Page)	La página a la que se accede en el servidor HTTP.
$pageCount	El número total de recursos descargados durante una prueba GETALL, excluyendo la propia página de prueba. Si la página probada no hace referencia a ningún otro recurso, este elemento no se genera.
$port*(Port)	Puerto utilizado para acceder al servidor HTTP. Si la prueba ha utilizado un servidor proxy, este es el valor del puerto del servidor proxy al cual se ha enviado la solicitud. Para conservar el puerto del servidor de destino previsto, establezca la propiedad generateProxyTokens en 1, o inicie el supervisor con el parámetro de la línea de mandatos -generateproxytokens
$previousChecksum	El elemento PreviousChecksum normalmente no proporciona valores significativos para clasificaciones de nivel de servicio porque los valores de suma de comprobación no se conocen cuando se crea el elemento de perfil (el supervisor calcula los valores de suma de comprobación mientras las pruebas están en progreso). Los elementos de supervisor $previousChecksum y $checksum están diseñados para el enriquecimiento de alertas utilizando el archivo de reglas del supervisor.
$proxyAuthType	El tipo de autenticación de servidor para el servidor proxy.
$proxyCache	El valor true indica que el servidor proxy ha recuperado la página web del servidor, en lugar de hacerlo desde su propia memoria caché.
$proxyPort	El número de puerto del servidor proxy al que se ha enviado la solicitud.
$proxyServer	El nombre de host del servidor proxy.
$proxyUsername	Lo utiliza el supervisor junto con la contraseña para iniciar la sesión en el servidor proxy.
$regexpMatch*n*	El contenido de la línea que coincide con la expresión regular.

Tabla 55. Elementos de supervisor HTTP (continuación)	
Elemento	**Descripción**
$regexp*n*	La expresión regular.
$regexpMatch*n*	El contenido de la línea que coincide con la expresión regular.
$regexpStatus*n*	El estado de la coincidencia de la expresión regular: NONE: no se configura ninguna comprobación de expresión regular. MATCHED: se ha encontrado una coincidencia para la expresión regular. FAILED: no se ha encontrado ninguna coincidencia para la expresión regular
$responsetime* (ResponseTime)	El tiempo que se tarda después de crear una conexión, hasta que se recibe el primer byte de la página.
$timeSinceModification	El tiempo que ha transcurrido desde que se modificó la página por última vez. Esta es la diferencia entre la hora de la prueba y el valor del campo de cabecera HTTP Last-Modified de la primera página recuperada.
$urlDownloadTimes*n** (UrlDownloadTime)	Tiempo de descarga de URL de cada elemento en una solicitud GETALL. Cada elemento se numera, empezando por 000 ($urlDownloadTime000, $urlDownloadTime001, $urlDownloadTime002 y, así, sucesivamente).
$url*n**(Url)	URL de cada página en una prueba GETALL. Cada página se numera, empezando por 000 ($url000, $url001, $url002 y, así, sucesivamente).
$urlResult*n** (UrlResultString)	Cadena de resultado para cada página descargada en una solicitud GETALL. Cada resultado se numera, empezando por 000 ($urlResult000, $urlResult001, $urlResult002, y, así, sucesivamente).
$username	El nombre utilizado para acceder a páginas que requieren que se autentique el usuario.

Mensaje de estado

El supervisor HTTP proporciona mensajes de estado en el atributo ResultMessage cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

Tabla 56. Tabla 4. Mensajes de estado de supervisor HTTP	
Mensaje	**Descripción**
Aceptar	La solicitud del supervisor se ha realizado correctamente.
Formulario no encontrado	No se ha podido encontrar la página requerida.
Inicializar captación de página ha fallado	No hay memoria suficiente para asignar espacio para el mecanismo de captación de página HTTP. El mensaje de la línea anterior debería contener más información.
La conexión ha fallado	El supervisor no se ha podido conectar por razones distintas a que el enlace está inactivo, que la conexión se restablece, que no se puede acceder al enlace, que la conexión ha agotado el tiempo de espera, que la conexión se ha terminado o que el host está inactivo. Consulte el archivo de registro del supervisor HTTP si desea más información.

Parámetros de formulario y coincidencia de expresión regular

Supervise el funcionamiento del formulario `http://support.mycompany.com/cgi-bin/search.cgi` enviando solicitudes HTTP POST con el parámetro de formulario `search=ism` y utilice una expresión regular para que coincida con la serie `Su búsqueda ha sido satisfactoria` en la respuesta. Si se devuelve esta cadena en la respuesta, clasifique el nivel de servicio como `Correcto` y, si no es así, como `Anómalo`.

Cree un nuevo elemento de perfil HTTP y establezca los campos tal como se muestra en la tabla siguiente.

Tabla 57. Ejemplo de elemento de perfil de formulario HTTP

Campo de configuración de elemento de perfil	**Valor**
server	`support.mycompany.com`
page	`/cgi-bin/search.cgi`
description	`Ejemplo - parámetros de formulario y expresiones regulares`
Detalles de expresión regular	
match 1	`Su búsqueda ha sido satisfactoria`
Detalles de clasificación de nivel de servicio	
statement	`Regexp Status 1 = MATCHED then status GOOD`
Detalles de cabecera y formulario	
name	`search`
value	`ism`
type	`FORM`

Propiedades

Las propiedades y las opciones de línea de mandatos específicas del supervisor HTTP se describen en la tabla siguiente.

Tabla 58. Propiedades de supervisor HTTP

Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
`AllowDuplicateDownload`	`0`|`1`	Forzar que se descarguen páginas cada vez que se encuentran. `0` - inhabilitado (descargado solo una vez) `1` - habilitado
`ForceHTMLParse`	`0`|`1`	Fuerza que las páginas que no tengan content-type `text/html` se analicen como HTML. `0` - inhabilitado `1` - habilitado

Tabla 58. Propiedades de supervisor HTTP (continuación)

Nombre de propiedad	Parámetro de propiedad	Descripción
GenerateProxyTokens	0|1	Especifica si el supervisor genera elementos adicionales que contengan información sobre el servidor proxy, si se utiliza un servidor proxy en una prueba. 0 - inhabilitado 1 - habilitado (los elementos adicionales $server y $port contienen valores para el servidor proxy)
GETALLThreadNum	1|2|3|4|5	Especifica el número de hebras separadas para utilizar durante una solicitud GETALL.
GetLinkTags	0|1	Activa la descarga de cinco hojas de estilo enlazadas para solicitudes GETALL. 0 - inhabilitado 1 - habilitado (si la página de destino contiene una etiqueta link con el valor de atributo rel=stylesheet, el supervisor intenta descargar el recurso al que hace referencia el atributo href de la etiqueta link)
HostnameLookupPreference	serie	Determina qué versión de IP, IPv6 o IPv4, se aplica al nombre de host proporcionado. Los valores posibles son: • 4Then6 selecciona IPv4 y, después, IPv6. Utiliza direcciones IPv4 si están disponibles. Si no se encuentra ninguna dirección IPv4, se utilizan direcciones IPv6. • 6Then4 seleccione IPv6 y, después, IPv4. Utiliza direcciones IPv6 si están disponibles. Si no se ha encontrado ninguna dirección IPv6, se utilizan direcciones IPv4. • 40nly solo selecciona IPv4. Solo utiliza direcciones IPv4. Si no hay ninguna dirección IPv4, el sondeo devuelve un error. • 60nly solo selecciona IPv6. Solo utiliza direcciones IPv6. Si no hay ninguna dirección IPv6, el sondeo devuelve un error. • 60r4 selecciona IPv4 o bien IPv6. Utiliza la primera dirección devuelta desde el nombre de host. Valor predeterminado: 4Then6
Ipv6Address	entero	La dirección local a la que se enlaza como origen para solicitudes HTTP cuando se utiliza HTTP IPv6. Valor predeterminado: sin dirección

Tabla 58. Propiedades de supervisor HTTP (continuación)		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
NoParseExtensions	serie	Una lista separada por comas de extensiones de archivo que indican los tipos de archivo que no analizará el supervisor y que en lugar de ello solo descargará.
OutputDirectory	serie	Especifica el directorio de salida para utilizar si OutputResult es true (establecido en 1). Valor predeterminado: $ISHOME/var
OutputResult	0|1	Especifica si el supervisor guarda los datos que recibe del servicio. 0 - inhabilitado 1 - habilitado
RelativeRedirects	0|1	Permite que los campos de ubicación de los códigos de estado HTTP 301 y HTTP 302 contengan URL relativos en lugar de URL absolutos. 0 - URL absolutos 1 - URL relativos
RFCPOST	0|1	Especifica que el supervisor debe seguir RFC1945 y RFC2616 y enviar un segundo POST después de una redirección. Muchos servidores web no esperan un POST después de una redirección y la mayoría de los navegadores no siguen las RFC. 0 - inhabilitado 1 - habilitado

Supervisor HTTPS

El supervisor HTTPS comprueba la disponibilidad y el tiempo de respuesta de servidores web. Puede supervisar páginas web individuales, incluidos los que utilizan formularios HTML, que normalmente requieren que el usuario especifique datos en campos.

Nota: El supervisor HTTPS funciona de la misma forma que el supervisor HTTP, pero se comunica con el servidor HTTP utilizando la versión 2 o la versión 3 del protocolo SSL (Secure Sockets Layer), que cifra todas las comunicaciones entre el servidor y el supervisor.

Tabla 59. Resumen de archivos de supervisor HTTPS	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	nco_m_https
Archivo de propiedades	$ISHOME/etc/props/https.props
Archivo de reglas	$ISHOME/etc/rules/https.rules
Archivo de registro	$ISHOME/log/https.log

Directrices para configurar el supervisor HTTPS

El supervisor HTTPS comprueba la disponibilidad y el tiempo de respuesta de servidores web. Utilice el supervisor HTTPS en las situaciones siguientes:

- El sitio web de destino es estático.

  Para sitios web dinámicos, utilice el supervisor TRANSX.
- Se presta servicio al sitio web de destino a través del protocolo HTTPS.

  Para sitios web que entregan contenido a través del protocolo HTTP, seleccione el supervisor HTTP.
- Para realizar la supervisión entre varias plataformas.
- Donde la velocidad es un factor determinante (el supervisor HTTPS proporciona un alto rendimiento).

Certificado del lado del cliente

El supervisor le permite supervisar servidores que requieren certificados del lado del cliente para una autenticación mutua.

Especifique el archivo de certificado SSL, el archivo de claves y la contraseña de clave al crear un elemento de perfil.

Los certificados deben estar en el formato PEM (Privacy Enhanced Mail). Si el certificado está en otro formato, debe convertirlo a formato PEM. Puede convertir certificados utilizando software como, por ejemplo, openSSL, que está disponible en http://www.openssl.org.

Nota: si utiliza siempre el mismo certificado, la misma clave y la misma contraseña en todos los elementos de perfil, especifíquelos utilizando propiedades de supervisor, en lugar de definiéndolas en cada elemento de perfil que cree.

Configuración de pruebas de servicio de supervisor HTTPS

Utilice los parámetros de configuración de supervisor HTTPS para definir pruebas de servicio HTTPS.

Tabla 60. Configuración de supervisor HTTPS

Campo	**Descripción**
server	Nombre de host del servidor que se va a supervisar. Por ejemplo, `www.myconpany.com`
page	URL de la página que se va a supervisar. Por ejemplo, `/secure/`
description	Campo de texto para proporcionar información descriptiva sobre el elemento.
port	Puerto del servidor que se va a utilizar. Valor predeterminado: 443
localip	Especifica la dirección IP de la interfaz de red que utiliza el supervisor para la prueba. Si este campo está en blanco, el supervisor utiliza la interfaz especificada por la propiedad `IpAddress`.
version	Versión del protocolo HTTPS que se va a utilizar: • `1.0` • `1.1` Valor predeterminado: `1.0`

Tabla 60. Configuración de supervisor HTTPS (continuación)	
Campo	**Descripción**
command	Tipo de solicitud: • HEAD • GET • GETALL • POST Valor predeterminado: GET
formname	Cuando se utiliza en una transacción, el supervisor HTTPS explora el formulario especificado para valores predeterminados. Los valores encontrados se llenan automáticamente en el siguiente paso HTTPS en la transacción.
authenticationtype	Especifica el mecanismo de autenticación de respuesta de verificación de identidad para autenticar usuarios de red: • NONE - Sin autenticación. • BASIC • NTLMv1 - Autenticación de respuesta de verificación de identidad de Windows NTLM versión 1. • NTLMv2 - Windows NTLM versión 2. Valor predeterminado: NONE
username	Nombre de usuario (nombre de cuenta) que el supervisor debe utilizar para iniciar sesión en el servidor HTTPS.
password	Contraseña correspondiente al nombre de usuario que el supervisor debe utilizar para iniciar sesión en el servidor.
sslcertificatefile	Vía de acceso y nombre de archivo del archivo de certificado digital utilizado en el elemento de supervisor. Si la vía de acceso no es absoluta, el supervisor lo interpreta como relativo al directorio de trabajo, ($ISMHOME/platform/arch/bin). Si no especifica un archivo de certificado, el supervisor utiliza el certificado especificado por la propiedad de supervisor SSLCertificateFile.
sslkeyfile	Vía de acceso y nombre de archivo del archivo que contiene la clave privada SSL, que se utiliza para identificar el servidor y firmar los mensajes SSL.
sslkeypassword	Contraseña utilizada para cifrar la clave privada SSL.
timeout	Tiempo de espera, en segundos, para que responda el servidor. Valor predeterminado: 30
poll	Tiempo, en segundos, entre cada sondeo. Valor predeterminado: 300

Tabla 60. Configuración de supervisor HTTPS (continuación)	
Campo	**Descripción**
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: `0`
retestinterval	Tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: `10`
Detalles de proxy	
server	Nombre de host del servidor proxy.
port	Puerto en el servidor proxy para utilizar.
authenticationtype	Tipo de autenticación de servidor para el servidor HTTPS de proxy. Consulte authenticationtype para obtener más información.
username	Nombre de usuario que debe utilizar el supervisor para iniciar sesión en el servidor HTTPS de proxy.
password	Contraseña que debe utilizar el servidor para iniciar sesión en el servidor HTTPS del proxy.
useproxy	Configura el supervisor para realizar la solicitud utilizando un servidor proxy. • `proxy` (utilizar `true` en ismbatch) • `noproxy` (utilizar `false` en ismbatch) El valor predeterminado es `noproxy`
hostnamelookuppreference	Determina qué versión de IP, IPv6 o IPv4, se aplica al nombre de host proporcionado. Las opciones son las siguientes: • `default` define el supervisor para utilizar valores de propiedades de nivel de supervisor. Es el valor predeterminado. • `4Then6` selecciona IPv4 y, después, IPv6. Utiliza direcciones IPv4 si están disponibles. Si no se encuentra ninguna dirección IPv4, se utilizan direcciones IPv6. • `6Then4` seleccione IPv6 y, después, IPv4. Utiliza direcciones IPv6 si están disponibles. Si no se ha encontrado ninguna dirección IPv6, se utilizan direcciones IPv4. • `4Only` solo selecciona IPv4. Solo utiliza direcciones IPv4. Si no hay ninguna dirección IPv4, el sondeo devuelve un error. • `6Only` solo selecciona IPv6. Solo utiliza direcciones IPv6. Si no hay ninguna dirección IPv6, el sondeo devuelve un error. • `6or4` selecciona IPv4 o bien IPv6. Utiliza la primera dirección devuelta desde el nombre de host.

Coincidencia de expresiones regulares

Puede realizar una búsqueda de expresiones regulares en la información que se está descargando especificando hasta 50 expresiones regulares diferentes. El supervisor HTTPS intenta hacer coincidir el contenido recuperado con cada una de las expresiones regulares.

Si se encuentra una coincidencia con una expresión regular especificada, las líneas que coinciden (o todas las que quepan en el almacenamiento intermedio interno del supervisor) se devuelven en el elemento `$regexpMatchn` correspondiente. Si la expresión regular coincide más de una vez en la información descargada, solo se devuelve la primera coincidencia. El estado de cada prueba de expresión regular se indica con los elementos `$regexpStatusn`. Puede utilizar las coincidencias de expresiones regulares y su información de estado como criterios para las clasificaciones del nivel de servicios.

Para obtener más información, consulte Tabla 50 en la página 338.

Parámetro de cabecera y formulario

Similar al supervisor HTTP, el supervisor HTTPS puede enviar datos adicionales en los campos de cabecera y el cuerpo del mensaje de solicitudes HTTP.

Si desea detalles sobre parámetros de cabecera y formulario, consulte Parámetro de cabecera y formulario HTTP.

Elementos de supervisor

Tabla 61. Elementos de supervisor SSL HTTPS

Elemento	Descripción
$SSLcertificateSerialNumber	Número de serie del certificado X509 presentado por el servidor.
$SSLcipherSuiteCount	Número de suites de cifrado disponibles en la conexión.
$SSLcipherSuiteList	Lista de suites de cifrado disponibles en la conexión.
$SSLcipherSuiteName	Suite de cifrado seleccionada para la conexión.
$SSLeffectiveSessionKeyBits	Número de bits en la clave de sesión. Normalmente, suele ser 128 o 168 o 40 para versiones de exportación.
$SSLHandshakeTime* (SslHandshakeTime)	Tiempo que se tarda en establecer la conexión SSL.
$SSLissuerName	Nombre del emisor para la certificación del formato X509 del servidor.
$SSLprotocolVersion	Versión de SSL que se está utilizando, v2 o v3.
$SSLpublicKeyLengthBits	Tamaño de la clave pública del servidor. Normalmente, suele ser 1024 bits, excepto cuando se utiliza una suite de cifrado de especificación de exportación.
$SSLserverCertificateValidFrom	Fecha a partir de la cual el certificado de servidor es válido.
$SSLserverCertificateValidTo	Fecha hasta la que el certificado de servidor es válido.
$SSLserverName	Nombre de servidor SSL.
$SSLsubjectName	Nombre del asunto para la certificación del formato X509. Normalmente, suele ser el nombre de la organización que controla el servidor.

Los elementos indicados con un asterisco (*) están disponibles como atributos. Los nombres de los atributos se muestran entre corchetes. La ausencia de un asterisco indica que no hay ningún atributo

equivalente. Los atributos que se muestran entre corchetes, pero sin elemento indican que solo están disponibles como atributos, no hay ningún elemento equivalente.

El supervisor HTTPS produce los mismos elementos adicionales que el supervisor HTTP, tal como se describe en Tabla 55 en la página 346. Además, genera los elementos relacionados con SSL si se utiliza un certificado del lado del cliente en la prueba, tal como se describe en Tabla 61 en la página 355.

Además de los resultados de pruebas comunes para todos los elementos, el supervisor HTTPS genera un conjunto de resultados de prueba que contienen datos específicos para pruebas de servicio HTTPS.

Mensaje de estado

El supervisor HTTPS proporciona mensajes de estado en el atributo `ResultMessage` cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

Además de los mensajes de estado HTTP, el supervisor HTTPS también genera los mensajes que se listan en Tabla 62 en la página 356.

Tabla 62. Mensajes de estado de supervisor HTTPS

Mensaje	Descripción
`CORRECTO`	El supervisor se ha conectado correctamente al servidor.
`El reconocimiento SSL ha fallado`	El supervisor no ha podido inicializar la conectividad SSL después de establecer una conexión con el servidor.
`Error de conexión`	El supervisor no se ha podido conectar por razones distintas a que el enlace está inactivo, que la conexión se restablece, que no se puede acceder al enlace, que la conexión ha agotado el tiempo de espera, que la conexión se ha terminado o que el host está inactivo. Consulte el archivo de registro del supervisor HTTP si desea más información.

Propiedades

El supervisor HTTPS tiene las mismas propiedades que el supervisor HTTP.

Si desea detalles sobre las opciones de propiedades que son las mismas que para el supervisor HTTP, consulte Tabla 58 en la página 349. La Tabla 5 lista algunas propiedades más específicas de HTTPS.

Tabla 63. Propiedades específicas de supervisor HTTPS

Nombre de propiedad	Parámetro de propiedad	Descripción
SSLCertificate File	serie	Vía de acceso y nombre de archivo del archivo de certificado digital que se utilizan si no se ha especificado ningún certificado de forma explícita para un elemento HTTPS durante su creación. Si la vía de acceso no es absoluta, el supervisor lo interpreta como relativo al directorio de trabajo, (`$ISHOME/platform/arch/bin`).
SSLCipherSuite	serie	Suite de cifrado que se utiliza para las operaciones SSL. Valor predeterminado: `RC4:3DES:DES:+EXP`

Tabla 63. Propiedades específicas de supervisor HTTPS (continuación)		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
SSLDisableTLS	entero	Inhabilita TLSv1 para el soporte de herencia. Valor predeterminado: 0 - TLSv1 está habilitado. 1 - TLSv1 está inhabilitado.
SSLKeyFile	serie	Archivo que contiene la clave privada SSL.
SSLKeyPassword	serie	Contraseña utilizada para cifrar la clave privada SSL.

Suites de cifrado

La propiedad SSLCipherSuite especifica la suite de cifrado utilizada el supervisor HTTPS. Para obtener más información sobre valores SSL, consulte "Establecimiento de SSL en Internet Service Monitoring" en la página 454.

Supervisor ICMP

El supervisor ICMP prueba el rendimiento del servicio del protocolo de mensajes de control de Internet que se ejecuta en una red. Para hacerlo, el supervisor utiliza el mandato de eco de ICMP.

En la tabla siguiente se enumeran los archivos de supervisor ICMP.

Tabla 64. Archivos de supervisor ICMP	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	nco_m_icmp
Archivo de propiedades	$ISHOME/etc/props/icmp.props
Archivo de reglas	$ISHOME/etc/rules/icmp.rules
Archivo de registro	$ISHOME/log/icmp.log

Directrices para configurar el supervisor ICMP

El supervisor ICMP emite solicitudes de eco de ICMP (normalmente denominadas pings) a los hosts de destino y espera una respuesta de solicitud de eco. Registra los tiempos de búsqueda, los tiempos de ida y vuelta y las métricas de índice de éxito que proporcionan una indicación del nivel de funcionamiento de la red. Cuando el supervisor emite una solicitud de eco, la solicitud puede pasar por uno o más direcciones antes de alcanzar el host de destino. Estos direccionadores pueden responder al supervisor antes de que el host de destino haya recibido la solicitud de eco. Si una solicitud de eco emitida por el supervisor pasa a través de un direccionador, el direccionador puede emitir una respuesta al supervisor. Esta respuesta podría indicar que el direccionador no ha podido localizar el host de destino, o que el direccionador está demasiado ocupado para procesar la solicitud. Es posible que el supervisor pueda recibir respuestas de varios direccionadores antes de recibir una respuesta de eco del host de destino. Si el supervisor recibe correctamente una respuesta de eco del host de destino, registra el tiempo que se ha tardado. Si el supervisor no recibe una respuesta del servidor de destino dentro del periodo de tiempo de espera especificado, la solicitud se registra como fallida. Puede configurar el supervisor para que envíe varias solicitudes de eco de ICMP al mismo destino en cada prueba. El supervisor registra estadísticas para cada una de las solicitudes enviadas.

Nota: Ejecute el supervisor ICMP como root porque abre un socket en bruto para enviar paquetes ICMP.

Configuración de pruebas de servicio de supervisor ICMP

Utilice los parámetros de configuración del supervisor ICMP para definir pruebas de servicio. Cuando configura el supervisor, se muestran los valores predeterminados para los parámetros de tiempo de

espera excedido e intervalo de sondeo, Estos valores predeterminados son 30 y 300 segundos, respectivamente. Los demás valores predeterminados que se listan en la tabla no se muestran durante la configuración, sino que se aplican al guardar los detalles de la configuración en caso de que no se especifique ningún valor.

La siguiente tabla lista las configuraciones del supervidor ICMP monitor.

Tabla 65. Configuración del supervisor ICMP

Campo	**Descripción**
server	Nombre de host o la dirección IP del servidor al que se envían las solicitudes de eco. Por ejemplo, `test.myconpany.com`
description	Campo de texto para proporcionar información descriptiva sobre el elemento.
timeout	Tiempo, en segundos, que se debe esperar a que responda el servidor a cada solicitud de eco. Valor predeterminado: `10`
numberofpings	Número de solicitudes de eco para enviar. Valor predeterminado: 5
packetinterval	Tiempo, en segundos, que se debe esperar entre el envío de solicitudes de eco. Valor predeterminado: 1
packetsize	Tamaño, en bytes, de cada solicitud de eco enviada. Valor predeterminado: 64
typeofservice	Define el campo Tipo de servicio en la capa IP. Se pueden especificar ambos valores, valores de tipo de servicio (TOS) de estilo IPv4 y valores de campo de servicio diferenciado DSCP. Los valores válidos son `0` -255.
retries	Número de veces que debe reintentar el supervisor cada solicitud de eco antes de abandonar. Valor predeterminado: `0`
poll	Tiempo, en segundos, entre cada sondeo. Valor predeterminado: `300`
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: `0`
retestinterval	Tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: `10`

Tabla 65. Configuración del supervisor ICMP (continuación)	
Campo	**Descripción**
hostnamelookuppreference	Determina qué versión de IP, IPv6 o IPv4, se aplica al nombre de host proporcionado. Las opciones son: • `default` define el supervisor para utilizar valores de propiedades de nivel de supervisor. Es el valor predeterminado. • 4Then6 selecciona IPv4 y, después, IPv6. Utiliza direcciones IPv4 si están disponibles. Si no se encuentra ninguna dirección IPv4, se utilizan direcciones IPv6. • 6Then4 seleccione IPv6 y, después, IPv4. Utiliza direcciones IPv6 si están disponibles. Si no se ha encontrado ninguna dirección IPv6, se utilizan direcciones IPv4. • `40nly` solo selecciona IPv4. Solo utiliza direcciones IPv4. Si no hay ninguna dirección IPv4, el sondeo devuelve un error. • `60nly` solo selecciona IPv6. Solo utiliza direcciones IPv6. Si no hay ninguna dirección IPv6, el sondeo devuelve un error. • `60r4` selecciona IPv4 o bien IPv6. Utiliza la primera dirección devuelta desde el nombre de host.

Nota: Supervise la disponibilidad del host `test.mycompany.com` comprobando los tiempos de respuesta en intervalos de 10 minutos. Intente conectarse al servidor en 30 segundos y, si el tiempo de espera se agota, vuelva a intentarlo dos veces más. Si sigue fallando, repita la prueba tres veces con 5 segundos entre cada reintento.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor ICMP genera un conjunto de resultados de pruebas que contienen datos específicos a pruebas de servicio ICMP.

En la tabla siguiente se describen los elementos adicionales para el supervisor ICMP.

Los elementos indicados con un asterisco (*) están disponibles como atributos. Los nombres de los atributos se muestran entre corchetes debajo del elemento. La ausencia de un asterisco indica que no hay ningún atributo equivalente. Los atributos que se muestran entre corchetes, pero sin un elemento indican que solo están disponibles como atributos, no hay ningún elemento equivalente.

Tabla 66. Elementos de supervisor ICMP	
Elemento	**Descripción**
`$averageRTT*(Average RTT)`	Tiempo medio de ida y vuelta en segundos.
`$endTime`	Hora de UNIX a la que se recibió la respuesta.
`$jitter`	Valor absoluto de la diferencia entre las horas de llegada de dos solicitudes de eco de ICMP adyacentes, menos sus horas de salida. Este valor se calcula de acuerdo con la fórmula especificada en RFC2598. El elemento se crea solo si el número de solicitudes de eco es mayor que uno. Si se utilizan más de dos solicitudes de eco, el valor es el jitter promedio entre todos los pares de solicitudes de eco.
`$lookupTime*(LookupTime)`	Tiempo que se tarda en obtener la dirección IP del servidor de host.
`$maxRTT*(MaxRTT)`	Tiempo máximo de ida y vuelta en segundos.

Tabla 66. Elementos de supervisor ICMP (continuación)	
Elemento	**Descripción**
$minRTT* (MinRTT)	Tiempo mínimo de ida y vuelta en segundos.
$numberPackets	Número de solicitudes de eco de ICMP enviadas, tal como se especifica en el elemento de perfil.
$packetInterval	Tiempo entre el envío de cada solicitud de eco de ICMP, tal como se especifica en el elemento de perfil.
$packetRetries	Número de veces que el supervisor ha intentado reenviar solicitudes de eco de ICMP antes de salir.
$packetSize	Tamaño (en bytes) de cada solicitud de eco de ICMP, tal como se especifica en el elemento de perfil.
$pingAttempts Failed	Número de intentos realizados para la primera solicitud de eco de ICMP incorrecta.
$pingAttempts Responded	Número de intentos realizados para la primera solicitud de eco de ICMP correcta.
$pingMessageFailed	Mensaje devuelto para la primera solicitud de eco de ICMP incorrecta.
$pingMessage Responded	Mensaje devuelto para la primera solicitud de eco de ICMP correcta.
$pingReceivedTime Failed	Hora UNIX a la que se recibió la primera respuesta de eco incorrecta.
$pingReceivedTime Responded	Hora UNIX a la que se recibió la primera respuesta de eco correcta.
$pingRespondIP Failed	Dirección IP que ha respondido a la primera solicitud de eco de ICMP incorrecta.
$pingRespondIP Responded	Dirección IP que ha respondido a la primera solicitud de eco de ICMP correcta.
$pingRTTFailed	Tiempo de ida y vuelta para la primera solicitud de eco de ICMP incorrecta en segundos.
$pingRTTResponded	Tiempo de ida y vuelta para la primera solicitud de eco de ICMP correcta en segundos.
$pingSentTime Failed	Hora UNIX a la que se envió la primera solicitud de eco de ICMP incorrecta.
$pingSentTime Responded	Hora UNIX a la que se envió la primera solicitud de eco de ICMP correcta.
$pingsFailed	Número de solicitudes de eco de ICMP enviadas para las que no había respuesta de eco.
$pingsResponded	Número de respuestas de eco válidas recibidas.
$pingTime	Tiempo que se tarda en recibir la respuesta de eco después de enviar la solicitud de eco de ICMP.
$respondPercent* (RespondPercent)	Porcentaje de solicitudes de eco de ICMP enviadas para las cuales había una respuesta.

Tabla 66. Elementos de supervisor ICMP (continuación)	
Elemento	**Descripción**
$responseTime	Tiempo que tarda el host de destino en responder a una solicitud de eco de ICMP.
$sentTime	Hora UNIX a la que se enviaron las solicitudes de eco de ICMP.
$spreadRTT	Diferencia entre $maxRTT y $minRTT.
$startTime	Hora UNIX a la que empezó la prueba.
$totalHostTime	Tiempo que se tarda en recibir la respuesta de eco después de iniciar la prueba.
$typeOfService	El campo Tipo de servicio en la capa IP, tal como se especifica al añadir un nuevo elemento ICMP. Para obtener detalles, consulte "Supervisor ICMP " en la página 357.

El supervisor ICMP crea un conjunto separado de elementos $pingname para registrar los resultados para cada solicitud de eco de ICMP enviada durante la prueba. El número de solicitudes enviadas se indica mediante $numberPackets. Por ejemplo, para el elemento $pingRTT, si $numberPackets es 3, el supervisor crea tres elementos ($pingRTT1, $pingRTT2 y $pingRTT3), que contienen la medida de tiempo de ida y vuelta para las tres solicitudes de eco de ICMP enviadas.

Mensaje de estado

El supervisor ICMP proporciona mensajes de estado en el atributo ResultMessage cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado ICMP.

Tabla 67. Mensajes de estado de supervisor ICMP	
Mensaje	**Descripción**
Pings completos	La solicitud de eco de ICMP se ha realizado correctamente.
Error de eco de ICMP	El supervisor no puede emitir la solicitud de eco de ICMP porque hay un problema con el host del supervisor o con su conexión con la red.
Tiempo de espera agotado	La solicitud de eco de ICMP ha agotado el tiempo de espera.
No localizable	Este mensaje se devuelve desde un direccionador y no siempre es preciso.
Reducción de origen	Un direccionador está demasiado ocupado para procesar la solicitud de eco de ICMP.
Tiempo excedido	Se devuelve este mensaje de un direccionador. Indica que la solicitud de eco de ICMP se ha reenviado alrededor de la red demasiadas veces.
Problema de parámetro	Se devuelve este mensaje de un direccionador. Indica que el direccionador no puede procesar la solicitud de eco de ICMP. Esto podría deberse a que el mensaje esté dañado.

Propiedades

Las propiedades especificas del supervisor ICMP se describen a continuación.

Tabla 68. Propiedades de ICMP		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
`EventsPerSec`	no aplicable	Esta propiedad no está soportada.
`IntraPingWait`	entero	Intervalo de tiempo mínimo en milisegundos entre todos los pings enviados por el supervisor ICMP. Se utiliza para ajustar el sistema para dispersar el tráfico de red durante un periodo de tiempo más largo. Por ejemplo, en un entorno con miles de hosts ICMP objetivo, establezca `IntraPingWait` en 3. Valor predeterminado: `0`
`Ipv6Address`	entero	Dirección local a la que enlazarse como origen para solicitudes de eco de ICMP al utilizar ICMP IPv6. Valor predeterminado: sin dirección
`MaxDNSResolvingThreads`	entero	Número máximo de hebras que utilizará el programa de resolución de DNS. Valor predeterminado: `20`
`MaxPacketSize`	entero	Tamaño máximo de paquete ICMP en bytes.
`PingsPerSec`	entero	Número de solicitudes de echo que intenta enviar el supervisor por segundo. El número de solicitudes reales enviadas depende de la carga de CPU y red. Valor predeterminado: `100`
`SocketBufferSize`	entero	Tamaño del almacenamiento intermedio de socket receptor (en kilobytes). Valor predeterminado: 32

Supervisor LDAP

El supervisor LDAP prueba el funcionamiento de lo servidores Lightweight Directory Access Protocol (LDAP).

En la tabla siguiente se listan los archivos del supervisor LDAP.

Tabla 69. Archivos del supervisor LDAP	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_ldap`
Archivo de propiedades	`$ISHOME/etc/props/ldap.props`
Archivo de reglas	`$ISHOME/etc/rules/ldap.rules`
Archivo de registro	`$ISHOME/log/ldap.log`

Directrices para configurar el supervisor LDAP

El supervisor LDAP prueba servicios LDAP conectándose con un servidor LDAP e intentando ubicar una entrada específica. Si el servidor consigue ubicar la entrada, devuelve el contenido de la entrada

al supervisor. El supervisor LDAP puede utilizar SSL para autenticarse y conectarse con el servidor LDAP.

Para configurar el supervisor LDAP es necesario comprender cómo funcionan el protocolo LDAP y el servicio de directorio supervisado. LDAP es un protocolo de Internet para acceder y gestionar servicios de directorio. Un servicio de directorio es una aplicación de base de datos distribuida. Un directorio consta de entradas. Por ejemplo, un directorio puede contener entradas relacionadas con los empleados o recursos de una organización. Cada entrada contiene un conjunto de atributos, por ejemplo las entrada de un directorio de empleados puede contener el nombre, el número de teléfono y la dirección de un empleado.

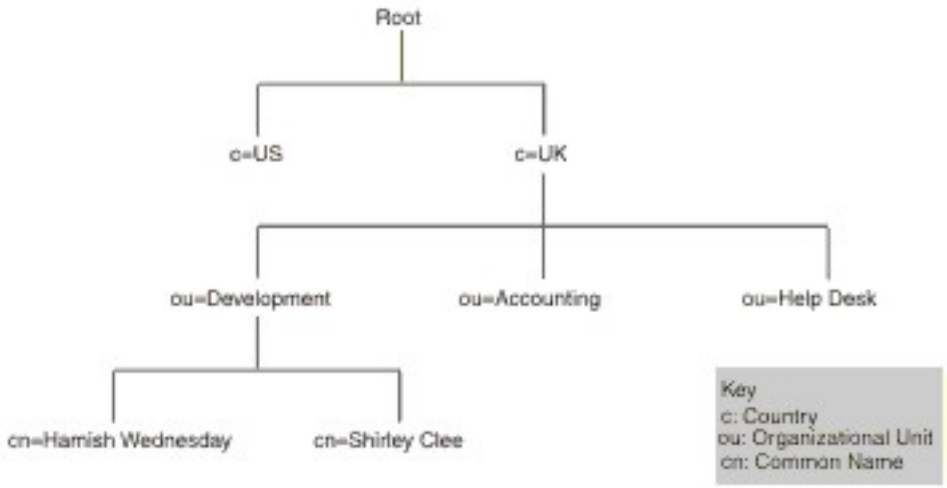
Los servicios de directorio individuales se pueden construir de forma diversa, por lo que el procedimiento de supervisión también puede diferir.

Versiones de LDAP

El supervisor LDAP admite tanto la versión 2 como la versión 3 de LDAP. De forma predeterminada, el supervisor intenta conectarse al servidor LDAP de destino que utiliza la versión 3 y, a continuación, retrocede automáticamente a la versión 2 si falla el intento. Puede forzar que el supervisor utilice siempre la versión 2 configurando la propiedad **NOLDAPV3**.

Servicio de directorio de ejemplo

Este servicio de directorio de ejemplo almacena los detalles personales de todos los empleados. El directorio se divide en países y luego en departamentos. Los empleados y sus atributos se almacenan en los departamentos correspondientes.



La imagen de ejemplo de jerarquía de directorios muestra un extracto de un directorio de ejemplo. Esta figura muestra una estructura de directorios. En el vértice, el nivel es root. Los dos subdirectorios representan países y están etiquetados como UK y US. El subdirectorio UK se divide en otros tres subdirectorios que representan las unidades organizativas. Están etiquetados como Development, Accounting y Help Desk. Dentro de la unidad organizativa Development, hay dos subdirectorios para nombres comunes, que son Shirley Clee y Hamish Wednesday.

A las entidades se hace referencia con sus nombres distinguidos. Un nombre distinguido es la ruta a la entidad. Por ejemplo, los nombres distinguidos del departamento de contabilidad (Accounting) y Hamish Wednesday serían:

```
dn="ou=accounting, c=UK"
dn="cn=Hamish Wednesday, ou=Development, c=UK"
```

La entrada para cada empleado tiene varios atributos. Por ejemplo, la entrada para Hamish Wednesday contiene los detalles siguientes.

```
cn: Hamish Wednesday
uid: ham
```

```
mail: HWednesday@development.mycompany.com
telephoneNumber: 88 88 55 44
```

Cada entidad de la jerarquía de directorios puede estar protegida por un nombre de usuario (en LDAP es un nombre distinguido) y una contraseña. El supervisor utiliza el nombre de usuario y contraseña para acceder al servidor LDAP.

Cuando el supervisor accede al servidor, indica dónde se inicia la búsqueda de la entidad de destino en la jerarquía de directorios. Esto se especifica en el campo searchBase como un nombre distinguido. Por ejemplo, la búsqueda podría empezar en el nivel de departamento.

```
ou=Accounting, c=UK
```

Nota: Las entidades que forman un nombre distinguido están en orden inverso. Es decir, se inician en el punto más bajo de la jerarquía y, a continuación, listan cada entidad anterior.

La entidad de destino se pasa al servidor en el campo de filtro. Este campo contiene un atributo de la entidad de destino. Por ejemplo, para buscar la entidad Hamish Wednesday's, el campo de filtro puede contener:

```
(uid=ham)
```

El servidor LDAP utiliza los campos suministrados por el supervisor para buscar la entidad de destino. El resultado de la búsqueda se devuelve al supervisor.

Si la búsqueda es correcta, el servidor también devuelve los atributos de la entidad de destino. El supervisor la convierte en elementos cuyos nombres se crean dinámicamente. Por ejemplo, el supervisor convertiría la entrada de Hamish Wednesday en:

```
$dnMatched = "cn=Hamish Wednesday, ou=Development, c=UK"
$cn = "Hamish Wednesday"
$uid = "ham"
$mail = "HWednesday@development.mycompany.com"
$telephoneNumber = "88 88 55 44"
```

Autenticación LDAP

La autenticación del servidor LDAP de SSL se basa en certificados de clave pública-privada firmados por entidades emisoras de certificados como, por ejemplo, Verisign y Thawte. Para la autenticación SSL, el supervisor LDAP utiliza la base de datos Netscape cert7db de certificados públicos para verificar las firmas de certificados de servidor emitidas por las autoridades certificadoras.

Si utiliza certificados firmados por una entidad emisora de certificados reconocida por Netscape como, por ejemplo, Verisign o Thawte, el supervisor LDAP los reconoce automáticamente. Si utiliza certificados firmados por su organización o por una organización que no está en la base de datos de Netscape, debe añadirlos a la base de datos cert7db.

Utilice el programa de utilidad certutil, disponible en Netscape, para añadir los certificados a la base de datos. La base de datos cert7db para el supervisor LDAP se encuentra en el archivo `$ISHOME/certificates/cert7.db`.

Para supervisar los servidores LDAP que están protegidos por el cifrado SSL o TLS, establezca las variables de entorno tal como se describe en la tabla siguiente:

Tabla 70. Variables de entorno necesarias para supervisar servidores LDAP seguros

Variable	Descripción	Valor
LDAPTLS_CACERT	Especifica el archivo que contiene los certificados CA	Archivo que contiene el certificado de servidor. Por ejemplo, `cacert.pem`.
LDAPTLS_REQCERT	Especifica las comprobaciones que hay que realizar en un certificado de servidor	Seleccione una de estas opciones: `never|allow|try|demand`.

Para obtener más información, consulte http://www.openldap.org.

Propiedades

Las propiedades específicas del supervisor LDAP se describen en la tabla siguiente:

Tabla 71. Opciones de propiedades del supervisor LDAP

Nombre de propiedad	Parámetro de propiedad	Descripción
NOLDAPV3	0|1	Fuerza al supervisor a utilizar LDAP v2 en lugar de LDAP v3. 0 - utilizar LDAP v3 1 - utilizar LDAP v2

Suites de cifrado

La propiedad `SSLCipherSuite` especifica la suite de cifrado utilizada el supervisor LDAP. Para obtener más información sobre valores SSL, consulte "Establecimiento de SSL en Internet Service Monitoring" en la página 454.

Configuración de pruebas de servicio de supervisor LDAP

Utilice los parámetros de configuración del supervisor LDAP para definir pruebas de servicios.

Cuando se configura el supervisor, el valor predeterminado mostrado para el parámetro de tiempo de espera es de 30 segundos y para el parámetro de intervalo de sondeo es de 300 segundos. Los demás valores predeterminados que se listan en la tabla no se muestran durante la configuración, sino que se aplican al guardar los detalles de la configuración en caso de que no se especifique ningún valor.

En la tabla siguiente se describen las configuraciones del supervisor LDAP:

Tabla 72. Configuración del supervisor LDAP

Campo	Descripción
server	El nombre o la dirección IP del servidor LDAP que se va a supervisar. Por ejemplo, `ldap.mycompany.in`.
searchbase	Nombre distinguido de la ubicación desde la que se va a iniciar la búsqueda. Por ejemplo, `ou=Accounting, c=UK`.
filter	Un atributo de la entidad de destino que se va a buscar. Por ejemplo, `(uid=ham)`.
description	Un campo de texto para proporcionar información descriptiva sobre el elemento. Por ejemplo, `Supervisor LDAP`.
Active	Selecciona si el elemento de perfil debe activarse después de crearlo. Por ejemplo, `Seleccionado`.
port	Puerto del servidor LDAP al que se va realizar la conexión. Debe especificar el puerto SSL si utiliza la autenticación SSL. Valor predeterminado: 389
username	El nombre de usuario utilizado para iniciar sesión en el servicio de directorio. El formato del nombre de usuario depende del valor de Tipo de autenticación. Puede especificar un dominio de Windows, es decir, `DOMAIN\username`. Por ejemplo, `jbloggs`.
password	La contraseña utilizada para iniciar sesión en el servicio de directorio, si es necesaria. Por ejemplo, `secret9`.

Tabla 72. Configuración del supervisor LDAP (continuación)	
Campo	**Descripción**
authenticationtype	El método de autenticación LDAP que se va a utilizar: • SIMPLE (contraseña de texto sin formato o anónima) • SSL-SIMPLE • SASL-DIGEST-MD5 **Nota:** La autenticación SASL-DIGEST-MD5 no está disponible en el sistema operativo Linux. Si establece authenticationtype en SIMPLE o SSL-SIMPLE, especifique el nombre de usuario en formato de nombre distinguido. Si establece authenticationtype en SASL-DIGEST-MD5, especifique el nombre de usuario como IDs de enlace SASL. Para iniciar la sesión en el servidor LDAP como usuario anónimo, establezca authenticationtype en SIMPLE y deje vacíos los campos de nombre de usuario y contraseña. Valor predeterminado: SIMPLE
saslrealm	El reino de autenticación del servidor LDAP; normalmente es el nombre completo de dominio del servidor. Si desea compartir contraseñas entre varios sistemas, puede utilizar un nombre de dominio. Por ejemplo, `miempresa.com`.
timeout	Tiempo de espera, en segundos, para que responda el servidor. Valor predeterminado: 30
poll	Tiempo, en segundos, entre cada sondeo. Valor predeterminado: 300
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: 0
retestinterval	Tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: 10

Clasificaciones de nivel de servicio

Las opciones de clasificación del nivel de servicio disponibles para el supervisor LDAP son:

```
totalTime
connectTime
searchTime
initTime
dnMatched
message
```

En las clasificaciones del nivel de servicio:

- Especifique clasificaciones de nivel de servicio adicionales especificando manualmente el nombre del elemento de supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección Elementos de supervisor.
- `message` puede ser cualquier mensaje que se reenvíe en el elemento **`$message`** al servidor IBM Application Performance Management si se utiliza en cualquier widget. Para obtener una lista de valores posibles, consulte Mensajes de estado.
- El operando es una serie o un número positivo.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor LDAP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio LDAP.

En la tabla siguiente se indican los elementos adicionales para el supervisor LDAP.

Tabla 73. Elementos del supervisor LDAP

Elemento	**Descripción**
$authentication	El tipo del método de autenticación de usuario necesario para el servidor LDAP (estándar o CRAM-MD5).
$connectTime* (ConnectTime)	Tiempo que se tarda en conectar con el servidor LDAP.
$distinguishedName* (UserName)	El nombre distinguido utilizado para iniciar sesión en el servicio de directorio.
$dnMatched	La entidad con la que se busca la coincidencia en la búsqueda.
$filter* (SrchFilter)	Atributo que se utiliza para buscar la entidad de destino.
$initTime* (InitTime)	Tiempo que se tarda en inicializar el cliente LDAP.
$port* (Port)	Puerto del servidor LDAP al que se ha conectado el supervisor.
$saslRealm	El reino SASL que ha especificado después de añadir un nuevo elemento LDAP.
$searchBase* (SearchBase)	El nombre distinguido de la entrada desde la cual se ha iniciado la búsqueda.
$searchTime* (SearchTime)	Tiempo que se tarda en completar la búsqueda.

Mensajes de estado

El supervisor LDAP proporciona mensajes de estado en el atributo **ResultMessage** cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado de LDAP.

Tabla 74. Mensajes de estado de supervisor LDAP

Mensaje	**Descripción**
`Búsqueda satisfactoria`	La solicitud se ha realizado correctamente.
`La búsqueda ha fallado`	La solicitud ha fallado

Tabla 74. Mensajes de estado de supervisor LDAP (continuación)	
Mensaje	**Descripción**
`Sin coincidencia`	Es posible que el servidor no encuentre una entrada coincidente en los criterios de búsqueda.
`La conexión ha agotado el tiempo de espera`	La conexión se ha establecido correctamente, pero el servidor ha dejado de responder.
`Inicialización fallida: se ha especificado un tipo de autenticación no reconocido`	Se produce si se utiliza un tipo de autenticación que el supervisor LDAP no soporta.
`La inicialización de cliente ha fallado`	La inicialización de las estructuras LDAP ha fallado debido a una memoria inadecuada.
`Ha fallado el enlace (autenticación)`	El servidor que está a la espera de que se complete el enlace ha excedido el tiempo de espera.
`El enlace SASL no es posible porque el servidor no admite LDAPv3`	El servidor debe dar soporte a LDAPv3 para crear un enlace SASL.
`El enlace SASL no es posible porque 'bind_id' (nombre de usuario), password o sasl_realm están en blanco`	Para que se produzca un enlace, todos los campos de autenticación deben tener un valor. Por tanto, un enlace SASL no es posible si el usuario ha iniciado sesión de forma anónima (en texto sin formato) utilizando el tipo de autenticación SIMPLE.
`Error de enlace SASL`	No se puede identificar el motivo de la anomalía de enlace SASL.
`Error de autorización de enlace SASL`	El enlace SASL ha fallado porque las credenciales de autorización eran incorrectas.

Supervisor IMAP4

El supervisor IMAP4 funciona con el supervisor SMTP para probar la disponibilidad y el tiempo de respuesta de un servicio de correo electrónico IMAP4.

En la tabla siguiente se listan los archivos de supervisor IMAP.

Tabla 75. Archivos de supervisor IMAP4	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_imap4`
Archivo de propiedades	`$ISHOME/etc/props/imap4.props`
Archivo de reglas	`$ISHOME/etc/rules/imap4.rules`
Archivo de registro	`$ISHOME/log/imap4.log`

Directrices para configurar el supervisor IMAP4

El supervisor IMAP4 funciona junto con el supervisor SMTP supervisando el buzón al que el supervisor SMTP envía los mensajes y midiendo la cantidad de tiempo que se tarda en entregar esos mensajes.

Nota: Asegúrese de que los relojes del sistema principal del supervisor y del servidor de correo estén sincronizados para que el cálculo de tiempo de entrega se realice correctamente.

Cuando el supervisor IMAP4 ha leído el contenido del buzón de correo, genera dos tipos distintos de sucesos:

- Sucesos específicos de mensajes

  El supervisor IMAP4 crea un suceso específico de mensaje para cada mensaje de correo electrónico que descarga del buzón. En este tipo de suceso, el supervisor establece el elemento `$message` en `Mensaje descargado correctamente`. El elemento `$timeToDeliver` se calcula como el tiempo necesario para que el mensaje vaya del supervisor SMTP que lo emitió al buzón que lo recibió. El elemento `$hopCount` indica el número de hosts que el mensaje se ha saltado para llegar al buzón.

- Sucesos de resumen

  El supervisor crea un suceso de resumen cuando ha procesado todos los mensajes del buzón. En este tipo de suceso, el elemento `$message` indica el número total de mensajes descargados correctamente desde el buzón y el elemento `$totaltime` indica el tiempo que se tarda en completar las solicitudes. El `$totaltime` está en segundos.

Correo seguro

El supervisor IMAP4 admite las conexiones con servicios de correo seguro. Se puede conectar utilizando SSL/TLS, o el mandato STARTTLS. Al definir un elemento de perfil, utilice el campo securitytype para seleccionar la seguridad apropiada. Si el servidor de correo requiere un certificado del lado del cliente para el cifrado SSL, utilice las propiedades SSL para especificar un archivo de certificado, un archivo de claves, una contraseña de clave y un conjunto cifrado.

Certificados del lado de cliente

El supervisor IMAP4 le permite supervisar servidores que requieren certificados del lado del cliente para la autenticación mutua.

Especifique el archivo de certificado SSL, el archivo de claves y la contraseña de clave al crear un elemento de perfil.

Los certificados deben estar en el formato PEM (Privacy Enhanced Mail). Si el certificado está en otro formato, debe convertirlo a formato PEM. Los certificados se pueden convertir utilizando software como, por ejemplo, openSSL, que está disponible desde http://www.openssl.org.

Nota: Si utiliza siempre el mismo certificado, la misma clave y la misma contraseña en todos los elementos de perfil, especifíquelos utilizando propiedades de supervisor, en lugar de definiéndolas en cada elemento de perfil que cree.

Buzones

Una vez que el supervisor IMAP4 ha procesado la información contenida en un mensaje de correo electrónico enviado por el supervisor SMTP, lo suprime del buzón. Puede utilizar cualquier buzón existente para almacenar los mensajes de correo electrónico entre los dos supervisores, incluso si el buzón pertenece a un usuario real. Sin embargo, es aconsejable crear una cuenta de buzón especial para la prueba de servicio.

Configuración de pruebas de servicio de supervisor IMAP4

Utilice los parámetros de configuración del supervisor IMAP4 para definir pruebas de servicio.

Cuando se configura el supervisor, los valores predeterminados se muestran para los parámetros de tiempo de espera y de intervalo de sondeo. Estos valores predeterminados son 30 y 300 segundos, respectivamente. Los demás valores predeterminados que se listan en la tabla no se muestran

durante la configuración, sino que se aplican al guardar los detalles de la configuración en caso de que no se especifique ningún valor.

Tabla 76. Configuración del supervisor IMAP4

Campo	Descripción
server	La dirección IP del servidor de correo. El ejemplo es `test.mycompany.com`
description	Campo de texto para proporcionar información descriptiva sobre el elemento.
port	El puerto IP del servidor IMAP4. Valor predeterminado: 143
securitytype	Tipo de conexión segura que se abre con el servidor de correo: • NONE: conectarse sin seguridad. • SSL: enviar hello de SSLv2 y luego negociar SSLv2, SSLv3 o TLSv1. • STARTTLS: conectarse sin seguridad, enviar un mandato STARTTLS, y luego establecer una conexión por TLSv1. Valor predeterminado: NONE
username	El nombre del buzón.
password	Contraseña que se utiliza para iniciar la sesión en el buzón, si fuese necesario.
authenticationtype	El método de autenticación para utilizar (STANDARD o CRAM_MD5) Valor predeterminado: STANDARD
sharedsecret	El secreto compartido para la autenticación CRAM_MD5, si procede.
timeout	El tiempo, en segundos, de espera a que responda el servidor. Valor predeterminado: 30
poll	El tiempo, en segundos, entre cada sondeo. Valor predeterminado: 300
failureretests	El número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: 0
retestinterval	El tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: 10

Coincidencia de expresiones regulares

Puede realizar una búsqueda de expresiones regulares en la información que se está descargando especificando hasta 50 expresiones regulares diferentes. El supervisor intenta hacer coincidir el contenido recuperado con cada una de las expresiones regulares.

Si se encuentra una coincidencia para cada una expresión regular especificada, las líneas coincidentes (o todas las que quepan en el almacenamiento intermedio del supervisor) se devuelven en el elemento `$regexpMatchn` correspondiente. Si la expresión regular coincide más de una vez en

la información descargada, sólo se devuelve la primera coincidencia. El estado de cada prueba de expresión regular se indica con los elementos $regexpStatusn. Puede utilizar las coincidencias de expresiones regulares y su información de estado como criterios para las clasificaciones del nivel de servicios.

Si desea más información sobre la sintaxis de la expresión regular, consulte Tabla 50 en la página 338.

Elementos de supervisor

Además de los resultados de pruebas comunes para todos los elementos, el supervisor IMAP4 genera un conjunto de resultados de prueba que contienen datos específicos para pruebas de servicio IMAP4.

En la tabla siguiente se describen los elementos adicionales para el supervisor IMAP4.

Los elementos indicados con un asterisco (*) están disponibles como atributos. Los nombres de los atributos se muestran entre corchetes. La ausencia de un asterisco indica que no hay ningún atributo equivalente. Los atributos que se muestran entre corchetes, pero sin un elemento indican que solo están disponibles como atributos, no hay ningún elemento equivalente.

Tabla 77. Elementos de supervisor IMAP4

Elemento	Descripción
$authentication	El tipo de método de autenticación de usuario necesario para el servidor IMAP4 (Estándar o CRAM-MD5).
$bytesPerSec	Número promedio de bytes transferidos cada segundo.
$bytesTransferred	El número de bytes cargados o descargados.
$connectTime	El tiempo que se tarda en conectarse al servidor IMAP4.
$downloadTime* (DownloadTime)	El tiempo que se tarda en descargar el archivo.
$hopCount	El número de hosts que ha saltado el mensaje para llegar al buzón.
$inEvent	Indica que este suceso forma parte de una serie de sucesos. 1 indica que no es el suceso final. 0 indica que es el suceso final.
$lookupTime*(LookupTime)	El tiempo que se tarda en obtener la dirección IP del servidor de host.
$port*(Port)	Puerto en que se supervisa el servicio.
$responseTime* (ResponseTime)	Tiempo entre el establecimiento de la conexión y la recepción del primer byte de datos.
$security	Tipo de conexión segura que se abre con el servidor de correo especificado al añadir un elemento IMAP (NONE, STARTTLS o SSL).
$sentTo*(SentTo)	La dirección de correo electrónico utilizada por el supervisor SMTP para enviar el mensaje original.
$smtpServer	El nombre del servidor SMTP desde el que se ha enviado el correo electrónico.
$SSLHandshakeTime* (SslHandshakeTime)	El tiempo que se tarda en establecer la conexión SSL.
$timeToDeliver	El tiempo que tarda un mensaje de correo electrónico en desplazarse entre un supervisor SMTP y su buzón de destino.

Tabla 77. Elementos de supervisor IMAP4 (continuación)	
Elemento	**Descripción**
$user*(ImapUser)	El nombre de usuario (nombre de cuenta) utilizado por el supervisor para iniciar la sesión en el servidor IMAP4.

Mensaje de estado

El supervisor IMAP proporciona mensajes de estado en el atributo ResultMessage cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado de IMAP4.

Tabla 78. Mensajes de estado de supervisor IMAP4	
Mensaje	**Descripción**
Mensaje descargado correctamente	El mensaje se ha descargado correctamente.
X mensajes descargados	Indica cuántos mensajes se han descargado correctamente del buzón.
El servidor no es compatible con IMAP4rev1	El servidor IMAP4 no cumple la especificación IMAP4 (RFC2060).
El servidor no admite la prestación STARTTLS	El servidor no se ha configurado correctamente.
No se puede iniciar sesión en el servidor	El supervisor no puede iniciar la sesión en el servidor IMAP.
Respuesta no reconocida para el mandato STATUS	El supervisor no reconoce el valor devuelto por el servidor.
Respuesta no reconocida para el mandato FETCH INTERNALDATE	
No se ha podido obtener la cabecera Actual-Time-Sent	El supervisor no ha obtenido la respuesta esperada del servidor.
No se ha podido obtener la cabecera Actually-To	
No se ha podido obtener la cabecera SMTP-Server	

Propiedades

Las propiedades y las opciones de línea de mandatos específicas del supervisor IMAP4 se describen en la tabla siguiente.

Tabla 79. Propiedades de supervisor IMAP4		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
`Originator`	serie	Especifica el campo De con el que se debe coincidir al recuperar mensajes de correo electrónico de prueba enviados por el supervisor SMTP. El supervisor recupera solo los mensajes donde el campo De coincide con la serie de Originator. Originator de IMAP4 debe coincidir con Originator en el supervisor SMTP. Valor predeterminado: `SMTP-Monitor`
`SSLCertificate File`	serie	La vía de acceso y el nombre de archivo del archivo de certificado digital utilizado si no se ha especificado ningún certificado de forma explícita para un elemento HTTPS durante su creación. Si la vía de acceso no es absoluta, el supervisor lo interpreta como relativo al directorio de trabajo, (`$ISHOME/platform/arch/bin`).
`SSLCipherSuite`	serie	La suite de cifrado que se utiliza para las operaciones SSL. Si desea una descripción de los valores posibles, consulte Suites de cifrado. Valor predeterminado: `RC4:3DES:DES:+EXP`
`SSLDisableTLS`	entero	Inhabilita TLSv1 para el soporte de herencia. Valor predeterminado: `0` - TLSv1 está habilitado. `1` - TLSv1 está inhabilitado.
`SSLKeyFile`	serie	El archivo que contiene la clave privada SSL.
`SSLKeyPassword`	serie	La contraseña utilizada para cifrar la clave privada SSL.

Suites de cifrado

La propiedad `SSLCipherSuite` especifica la suite de cifrado utilizada por el supervisor IMAP4. Para más información sobre valores SSL, consulte “Establecimiento de SSL en Internet Service Monitoring” en la página 454.

Supervisor NTP

El supervisor NTP (protocolo de hora en red) consulta un servidor NTP utilizando UDP (User Datagram Protocol) para determinar si el servidor está suministrando la hora correcta.

NTP utiliza la Hora Universal Coordinada para sincronizar los relojes de sistema al milisegundo.

En la tabla siguiente se enumeran los archivos de supervisor NTP.

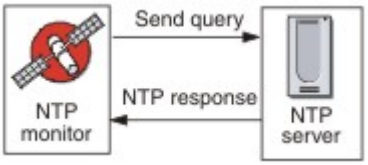
Tabla 80. Archivos del supervisor NTP	
Archivos de supervisor	**Nombre y ubicación**
Archivo ejecutable de supervisor	`nco_m_ntp`
Archivo de propiedades	`$ISHOME/etc/props/ntp.props`
Archivo de reglas	`$ISHOME/etc/ntp.rules`

Tabla 80. Archivos del supervisor NTP (continuación)	
Archivos de supervisor	**Nombre y ubicación**
Archivo de registro	`$ISHOME/log/ntp.log`

Directrices para configurar el supervisor NTP

El supervisor NTP adquiere datos enviando una consulta a un servidor NTP, que devuelve un paquete de respuestas UDP con la hora actual (tal como ve el servidor NTP).

La imagen siguiente muestra un ejemplo de los mensajes que se intercambian entre el supervisor y el servidor NTP.



Configuración de pruebas de servicio de supervisor NTP

Utilice los parámetros de configuración del supervisor NTP para definir pruebas de servicios.

En la tabla siguiente se describen las configuraciones de NTP:

Tabla 81. Configuración NTP	
Campo	**Descripción**
server	Nombre de host del servidor NTP. Por ejemplo, `ntp.mycompany.com`.
description	Campo de texto para proporcionar información descriptiva sobre el elemento. Por ejemplo, `Supervidor NTP`.
port	Puerto del servidor NTP que se va a utilizar. Valor predeterminado: `123`
localip	Especifica la dirección IP de la interfaz de red en el sistema host al que se enlaza el supervisor cuando realizar la prueba. Si se configura la propiedad `IpAddress` del supervisor, sustituye el valor de este campo. Por ejemplo, `102.168.n.n`.
version	Versión del servidor NTP que se va a utilizar (1, 2, 3 o 4). Valor predeterminado: `1`
timeout	Tiempo de espera, en segundos, para que responda el servidor. Valor predeterminado: `10`
retries	Número de veces que el supervisor vuelve a intentar contactar con el servidor NTP. Valor predeterminado: `0`
poll	Tiempo, en segundos, entre cada sondeo. Valor predeterminado: `300`

Tabla 81. Configuración NTP (continuación)	
Campo	**Descripción**
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: `0`
retestinterval	Tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: `10`

Clasificación de nivel de servicio

Las clasificaciones del nivel de servicio definen las reglas para determinar el nivel de servicio que se suministra a través de NTP.

Las opciones de clasificación del nivel de servicio disponibles para el supervisor NTP son estas:

```
totalTime
responseTime
lookupTime
offset
adjustedOffset
message
```

En las clasificaciones del nivel de servicio:

- Especifique más clasificaciones de nivel de servicio entrando manualmente el nombre del elemento supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección Elementos de supervisor.
- `message` puede ser cualquier mensaje que se reenvíe en el elemento `$message` al servidor IBM Application Performance Management si se utiliza en cualquier widget. Para obtener una lista de valores posibles, consulte Mensajes de estado.
- El operando es una serie o un número positivo.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor NTP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio NTP.

En la tabla siguiente se describen los elementos adicionales para el supervisor NTP.

Tabla 82. Elementos del supervisor NTP	
Elemento	**Descripción**
`$adjustedOffset`	Lapso temporal con respecto al servidor en segundos.
`$localIP`	Dirección IP local configurada para ser utilizada por el supervisor. Puede estar en blanco en un sistema con una sola interfaz.
`$lookupTime*` (`LookupTime`)	Tiempo que se tarda en obtener la dirección IP del servidor de host.
`$ntpVersionIn`	Versión de protocolo utilizada en la respuesta del servidor.
`$ntpVersionOut`	Versión de protocolo utilizada para el envío.

Tabla 82. Elementos del supervisor NTP (continuación)	
Elemento	**Descripción**
`$offset`	Lapso temporal entre el servidor NTP y el sistema que ejecuta el supervisor en segundos.
`$port*` (`Port`)	Puerto del servidor NTP que se va a utilizar.
`$responseTime*` (`ResponseTime`)	Tiempo transcurrido entre la conexión al servidor NTP por parte del supervisor y la recepción de una respuesta.
`$retries`	Número de veces que se reenvía una solicitud si no se reciben ID de respuesta.

Mensajes de estado

El supervisor NTP proporciona mensajes de estado en el atributo `ResultMessage` cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado de NTP.

Tabla 83. Mensajes de estado del supervisor NTP	
Mensaje	**Descripción**
`Successful query` (Consulta satisfactoria)	El servidor NTP ha dado la respuesta esperada.
`Connection failed` (Error de conexión)	No se puede inicializar un socket UDP.
`Failed to send request to NTP server` (No se ha podido enviar solicitudes al servidor NTP)	No se ha podido escribir en el socket UDP.
`No response from server` (No hay respuesta del servidor)	El servidor NTP no ha respondido.

Supervisor NNTP

El supervisor NNTP prueba la disponibilidad de un servicio NNTP leyendo de un grupo de noticias y publicando en el mismo.

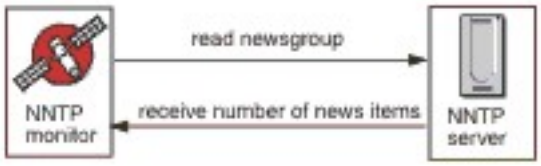
En la tabla siguiente se enumeran los archivos de supervisor NNTP.

Tabla 84. Archivos del supervisor NNTP	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_nntp`
Archivo de propiedades	`$ISHOME/etc/props/nntp.props`
Archivo de reglas	`$ISHOME/etc/rules/nntp.rules`
Archivo de registro	`$ISHOME/log/nntp.log`

Directrices para configurar el supervisor NNTP

El supervisor NNTP prueba los servicios NNTP enviándolos a un servidor NNTP y leyendo de ellos. Cada elemento de perfil que cree para el supervisor realiza una operación de lectura o una operación de envío.

En una operación de lectura, el supervisor se conecta al servicio NNTP para comprobar si existe un grupo de noticias de Internet determinado. Si el grupo de noticias existe, el supervisor registra el número de elementos de noticias que incluye. También intenta registrar el último elemento de noticias añadido al grupo de noticias. La imagen siguiente muestra la operación de lectura.



En una operación de envío, el supervisor comprueba que el grupo de noticias exista y luego intenta escribir un mensaje de prueba. El asunto del mensaje de texto es `NNTP Monitor Test Message` (mensaje de prueba del supervisor NNTP). En la imagen siguiente se muestra la operación de envío.

Cada elemento de perfil especifica un nombre de usuario (`username`) y una contraseña `password` suministrados por el supervisor cuando accede a un servidor NNTP. El supervisor utiliza el sistema de autenticación de texto sin formato.

```
AUTHINFO USER username
AUTHINFO PASS password
```

Donde `username` y `password` se especifican en el elemento de perfil de supervisor.

Propiedades

Las opciones de propiedades específicas para el supervisor NNTP se describen en la tabla siguiente.

Tabla 85. Opciones de propiedades del supervisor NNTP

Nombre de propiedad	Parámetro de propiedad	Descripción
OutputDirectory	serie	Especifica el directorio de salida para utilizar si **`OutputResult`** es true (establecido en 1). Valor predeterminado: `$ISHOME/var`
OutputResult	0|1	Especifica que el supervisor puede guardar los datos que recibe del servicio. 0 - inhabilitado 1 - habilitado

Configuración de pruebas de servicio de supervisor NNTP

Utilice los parámetros de configuración del supervisor NNTP para definir pruebas de servicios.

En la tabla siguiente se listan las configuraciones del supervisor NNTP.

Tabla 86. Configuración del supervisor NNTP	
Campo	**Descripción**
server	La dirección IP del servidor NNTP. Por ejemplo, `news.mycompany.com`.
newsgroup	Nombre del grupo de noticias que utiliza el supervisor para publicar y leer mensajes de prueba. Por ejemplo, `mycompany.test`.
description	Un campo de texto para proporcionar información descriptiva sobre el elemento. Por ejemplo, LECTURA.
port	El número de puerto del servidor NNTP. Valor predeterminado: `119`
username	Nombre de usuario que se utiliza para la autenticación con el servidor NNTP.
password	Contraseña del nombre de usuario que se utiliza para la autenticación con el servidor NNTP.
action	Indica si se debe publicar o recuperar un artículo. Puede ser READ o POST. Valor predeterminado: POST
timeout	El tiempo de espera, en segundos, para que responda el servidor. Valor predeterminado: `30`
poll	El tiempo, en segundos, entre cada sondeo. Valor predeterminado: `300`
failureretests	El número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: `0`
retestinterval	El tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: `10`

Coincidencia de expresiones regulares

Puede realizar una búsqueda de expresiones regulares en la información que se está descargando especificando hasta 50 expresiones regulares diferentes. El supervisor NNTP intenta hacer coincidir el contenido recuperado con cada una de las expresiones regulares.

Si se encuentra una coincidencia para cada una expresión regular especificada, las líneas coincidentes (o todas las que quepan en el almacenamiento intermedio del supervisor) se devuelven en el elemento `$regexpMatchn` correspondiente. Si la expresión regular coincide más de una vez en la información descargada, sólo se devuelve la primera coincidencia. El estado de cada prueba de expresión regular se indica con los elementos `$regexpStatusn`. Puede utilizar las coincidencias de expresiones regulares y su información de estado como criterios para las clasificaciones del nivel de servicios.

Para obtener más información, consulte Tabla 50 en la página 338.

Clasificaciones de nivel de servicio

Las clasificaciones del nivel de servicio definen las reglas para determinar el nivel de servicio que se suministra a través de NNTP.

Las opciones de clasificación del nivel de servicio disponibles para el supervisor NNTP son estas:

```
totalTime
lookupTime
connectTime
transferTime
responseTime
estatus
bytesTransferred
bytesPerSec
newsItems
expected
lastLineReceived
checksum
previousChecksum
regexpMatch1 a 3
regexpStatus1 a 3
mensaje
```

En las clasificaciones del nivel de servicio:

- Especifique más clasificaciones de nivel de servicio entrando manualmente el nombre del elemento supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección Elementos de supervisor.
- `message` puede ser cualquier mensaje que se reenvíe en el elemento `$message` al servidor IBM Application Performance Management si se utiliza en un widget. Para obtener una lista de valores posibles, consulte Mensajes de estado.
- El operando es una serie o un número positivo.
- Los códigos de `status` `220` y `240` indican que ha sido satisfactorio. Consulte el protocolo NNTP para ver otros códigos de estado devueltos por la operación.
- `egexpStatus`*n* puede tener los valores siguientes:
  - `NONE`: no se configura ninguna comprobación de expresión regular.
  - `MATCHED`: se ha encontrado una coincidencia para la expresión regular.
  - `FAILED`: no se ha encontrado una coincidencia para la expresión regular.
- Evaluación de coincidencia de expresiones regulares que utilizan expresiones de prueba con el formato:

  ```
  regexpMatchn
  [contains|!contains] expresión
  ```

  Utilice los operadores `contains` y `!contains` en lugar de = y `!=`, ya que `regexpMatch`*n* contiene normalmente toda la línea que coincide con la expresión regular en lugar de sólo la parte coincidente, por lo que los operadores = y `!=` a menudo no coinciden con la expresión.
- Los elementos `Checksum` y `PreviousChecksum` no suelen proporcionar valores significativos para las clasificaciones del nivel de servicio porque los valores de la suma de comprobación no se conocen cuando se crea el elemento del perfil (el supervisor calcula los valores de la suma de comprobación mientras hay pruebas en progreso). Los elementos de supervisor `$checksum` y `$previousChecksum` están pensados para el enriquecimiento de alertas mediante el archivo de reglas del supervisor.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor NNTP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio NNTP.

En la tabla siguiente se describen los elementos adicionales para el supervisor NNTP.

Tabla 87. Elementos del supervisor NNTP	
Elemento	**Descripción**
$action* (NntpAction)	Acción que lleva a cabo el supervisor. Puede ser READ o POST.
$bytesPerSec	Número promedio de bytes transferidos cada segundo.
$bytesTransferred	El número de bytes cargados o descargados.
$checksum	El elemento Checksum no suele proporcionar valores significativos para las clasificaciones del nivel de servicio porque los valores de la suma de comprobación no aparecen cuando el elemento de perfil se crea (el supervisor calcula los valores de la suma de comprobación mientras las pruebas están en progreso). Los elementos de supervisor $checksum y $previousChecksum están pensados para el enriquecimiento de alertas mediante el archivo de reglas del supervisor.
$connectTime* (ConnectTime)	El tiempo que se tarda en establecer una conexión con el servidor NNTP.
$downloadTime	El tiempo que se tarda en descargar el archivo.
$group* (NntpGroup)	Nombre del grupo de noticias supervisado.
$lastLineReceived	Este elemento sólo se configura si el elemento $message contiene el mensaje Expect Failed. Si se establece, contiene la respuesta del servidor NNTP.
$lookupTime* (LookupTime)	El tiempo que se tarda en buscar la dirección IP del servidor.
$newsItems	El número de elementos nuevos del grupo de noticias.
$password	La contraseña utilizada para autenticar el supervisor.

Tabla 87. Elementos del supervisor NNTP (continuación)	
Elemento	**Descripción**
$previousChecksum	El elemento PreviousChecksum no suele proporcionar valores significativos para las clasificaciones del nivel de servicio porque los valores de la suma de comprobación no aparecen cuando el elemento de perfil se crea (el supervisor calcula los valores de la suma de comprobación mientras las pruebas están en progreso). Los elementos de supervisor $previousChecksum y $checksum están pensados para el enriquecimiento de alertas mediante el archivo de reglas del supervisor.
$responseTime* (ResponseTime)	El tiempo necesario, después de la creación de una conexión, hasta que se reciba el primer byte del artículo de destino.
$status	El código de estado devuelto por el servidor NNTP.
$transferTime* (TransferTime)	Establece el valor en $uploadTime o $downloadTime.
$uploadTime	El tiempo que se tarda en cargar el archivo.
$username	El nombre de usuario utilizado para autenticar el supervisor.
Si $message contiene $ExpectFailed	
$expected	El texto de la conexión que esperaba el supervisor para cuando falló la conexión.
$lastLineReceived	La última línea de texto en la conexión que ha recibido el supervisor desde el servidor NNTP.

Mensajes de estado

El supervisor NNTP proporciona mensajes de estado en el atributo ResultMessage cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado de NNTP.

Tabla 88. Mensajes de estado del supervisor NNTP	
Mensaje	**Descripción**
Article Posted (Artículo enviado)	La acción POST de NNTP se ha realizado correctamente.
Article Retrieved (Artículo recuperado)	La acción READ de NNTP se ha realizado correctamente.
Not Found (No encontrado)	Es posible que el artículo no se haya localizado.

Tabla 88. Mensajes de estado del supervisor NNTP (continuación)	
Mensaje	**Descripción**
`Expect failed` (Fallo esperado)	Ha fallado la solicitud NNTP.
`Timed out waiting to read` (Tiempo de espera excedido al esperar la lectura)	Se ha establecido una conexión de datos con el servidor, pero ha dejado de responder.
`Connection failed` (Error de conexión)	El supervisor no ha podido conectarse al servidor. Para obtener más información, consulte el archivo de registro.
`Connection closed by foreign host` (Conexión cerrada por host foráneo)	El host remoto ha cerrado la conexión antes de lo que esperaba el supervisor.

Supervisor POP3

El supervisor POP3 funciona junto con el supervisor SMTP para probar la disponibilidad y el tiempo de respuesta de un servicio de correo electrónico POP3.

En la tabla siguiente se listan los archivos de supervisor POP3.

Tabla 89. Archivos del supervisor POP3	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_pop3`
Archivo de propiedades	`$ISHOME/etc/props/pop3.props`
Archivo de reglas	`$ISHOME/etc/rules/pop3.rules`
Archivo de registro	`$ISHOME/log/pop3.log`

Directrices para configurar el supervisor POP3

El supervisor POP3 funciona junto con el supervisor SMTP supervisando el buzón al que el supervisor SMTP envía los mensajes y midiendo la cantidad de tiempo que se tarda en entregar esos mensajes.

Nota: Asegúrese de que los relojes del sistema principal del supervisor y del servidor de correo estén sincronizados para que el cálculo de tiempo de entrega se realice correctamente.

Una vez que el supervisor POP3 ha leído el contenido del buzón, genera dos tipos de sucesos diferentes:

- Sucesos específicos de mensajes

  El supervisor POP3 crea un suceso específico de mensaje para cada mensaje de correo electrónico que descarga del buzón. En este tipo de suceso, el supervisor establece el elemento `$message` en `Mensaje descargado correctamente`. El elemento `$timeToDeliver` se calcula como el tiempo necesario para que el mensaje vaya del supervisor SMTP que lo emitió al buzón que lo recibió. El elemento `$hopCount` indica el número de hosts que el mensaje se ha saltado para llegar al buzón.
- Sucesos de resumen

  El supervisor crea un suceso de resumen cuando ha procesado todos los mensajes del buzón. En este tipo de suceso, el elemento `$message` indica el número total de mensajes descargados correctamente desde el buzón y el elemento `$totaltime` indica el tiempo que se tarda en completar las solicitudes. El `$totaltime` está en segundos.

Correo seguro

El supervisor POP3 admite conexiones a servicios de correo seguro. Se puede conectar utilizando SSL/TLS, o el mandato STARTTLS. Cuando defina un elemento del supervisor POP3, utilice el campo de Tipo de seguridad para seleccionar la seguridad adecuada. Si el servidor de correo requiere un certificado del lado del cliente para el cifrado SSL, utilice las propiedades o las opciones de la línea de mandatos de SSLname para especificar un archivo de certificado, un archivo de claves, una contraseña de clave y una suite de cifrado.

Certificado del lado del cliente

El supervisor POP3 le permite supervisar servidores que requieren certificados del lado del cliente para la autenticación mutua. Al crear un elemento de perfil, especifique el archivo de certificados SSL, el archivo de claves y la contraseña de clave. Los certificados deben estar en el formato PEM (Privacy Enhanced Mail). Si su certificado está en otro formato, deberá convertirlo al formato PEM. Puede convertir certificados utilizando software como, por ejemplo, openSSL, que está disponible en http://www.openssl.org.

Nota: Si utiliza siempre el mismo certificado, la misma clave y la misma contraseña en todos los elementos de perfil, especifíquelos utilizando propiedades de supervisor en lugar de definiéndolos en cada elemento de perfil que cree.

Configuración de las pruebas de servicios del supervisor POP3

Nota: Supervise la operación del servidor de correo `mail.mycompany.com` configurando el supervisor SMTP para enviar mensajes a una bandeja de correo de prueba test y configurando el supervisor POP3 para que recupere los mensajes. El buzón de prueba tiene la dirección `ismtest@mycompany.com` y las credenciales `ismtest/secret1`. Utilice un tiempo de espera de conexión de 20 segundos, 2 repeticiones de pruebas tras anomalías y un intervalo de repetición de pruebas de 5 segundos en cada extremo, y pruebe los servicios cada diez minutos. Utilice las clasificaciones de nivel de servicio predeterminadas que proporcionan los elementos de perfil.

Tabla 90. Configuración del supervisor POP3

Campo	**Descripción**
server	La dirección IP del servidor de correo. El ejemplo es `mail.mycompany.com`
description	Un campo de texto para proporcionar información descriptiva sobre el elemento.
port	Número de puerto del servidor de correo. Valor predeterminado: `110`
securitytype	Tipo de conexión segura que se abre con el servidor de correo: • `NONE`: conectarse sin seguridad. • `SSL`: enviar `hello` de SSLv2 y luego negociar SSLv2, SSLv3 o TLSv1. • `STARTTLS`: conectarse sin seguridad, enviar un mandato STLS, y luego establecer una conexión por TLSv1. Este es el tipo de seguridad más seguro. • `NONE`: conectarse sin seguridad. Valor predeterminado: `NONE`
username	El nombre del buzón.
password	Contraseña que se utiliza para iniciar la sesión en el buzón, si fuese necesario.

Tabla 90. Configuración del supervisor POP3 (continuación)	
Campo	**Descripción**
authenticationtype	El método de autenticación que se debe utilizar y la etiqueta es Tipo de autenticación: • /TANDARD: utiliza un intercambio de usuario/contraseña en el que la contraseña no está cifrada. Es adecuado para el uso intermitente de POP3. • APOP: se utiliza cuando el cliente POP3 se conecte regularmente con el servidor. Ofrece un mayor nivel de seguridad que el método estándar. Asegúrese de especificar un secreto compartido APOP si selecciona APOP. Tenga en cuenta que no todos los servidores admiten APOP. Valor predeterminado: STANDARD.
sharedsecret	Secreto compartido para la autenticación APOP. Sólo se aplica si se utiliza el tipo de autenticación APOP. La cadena debe tener una longitud de al menos ocho caracteres y está oculta en la interfaz de usuario.
timeout	El tiempo, en segundos, de espera a que responda el servidor. Valor predeterminado: 30
poll	El tiempo, en segundos, entre cada sondeo. Valor predeterminado: 300
failureretests	El número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: 0
retestinterval	El tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: 10
verifycertificate	Certificado de verificación del servidor. Valor predeterminado: Disabled

Utilice los parámetros de configuración del supervisor POP3 para definir pruebas de servicios.

Coincidencia de expresiones regulares

Puede realizar una búsqueda de expresiones regulares en la información que se está descargando especificando hasta 50 expresiones regulares diferentes. El supervisor intenta hacer coincidir el contenido recuperado con cada una de las expresiones regulares.

Si se encuentra una coincidencia para cada una expresión regular especificada, las líneas coincidentes (o todas las que quepan en el almacenamiento intermedio del supervisor) se devuelven en el elemento `$regexpMatchn` correspondiente. Si la expresión regular coincide más de una vez en la información descargada, sólo se devuelve la primera coincidencia. El estado de cada prueba de expresión regular se indica con los elementos `$regexpStatusn`. Puede utilizar las coincidencias de expresiones regulares y su información de estado como criterios para las clasificaciones del nivel de servicios.

Si desea más información sobre la sintaxis de la expresión regular, consulte Tabla 50 en la página 338.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor POP3 genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio POP3.

En la tabla 1 se describen los elementos adicionales para el supervisor POP3.

Los elementos indicados con un asterisco (*) están disponibles como atributos. Los nombres de los atributos se muestran entre corchetes. La ausencia de un asterisco indica que no hay ningún atributo equivalente. Los atributos que se muestran entre corchetes, pero sin un elemento indican que solo están disponibles como atributos, no hay ningún elemento equivalente.

Tabla 91. Elementos de supervisor IMAP4

Elemento	Descripción
$authentication	El tipo de método de autenticación de usuario necesario para el servidor IMAP4 (Estándar o CRAM-MD5).
$bytesPerSec	Número promedio de bytes transferidos cada segundo.
$bytesTransferred	El número de bytes cargados o descargados.
$connectTime	El tiempo que se tarda en conectarse al servidor IMAP4.
$downloadTime* (DownloadTime)	El tiempo que se tarda en descargar el archivo.
$hopCount	El número de hosts que ha saltado el mensaje para llegar al buzón.
$inEvent	Indica que este suceso forma parte de una serie de sucesos. 1 indica que no es el suceso final, 0 indica que es el suceso final.
$lookupTime*(LookupTime)	El tiempo que se tarda en obtener la dirección IP del servidor de host.
$port*(Port)	Puerto en que se supervisa el servicio.
$responseTime*(ResponseTime)	Tiempo entre el establecimiento de la conexión y la recepción del primer byte de datos.
$security	Tipo de conexión segura que se abre con el servidor de correo especificado al añadir un elemento IMAP (NONE, STARTTLS o SSL).
$sentTo*(SentTo)	La dirección de correo electrónico utilizada por el supervisor SMTP para enviar el mensaje original.
$smtpServer	El nombre del servidor SMTP desde el que se ha enviado el correo electrónico.
$SSLHandshakeTime* (SslHandshakeTime)	El tiempo que se tarda en establecer la conexión SSL.
$timeToDeliver	El tiempo que tarda un mensaje de correo electrónico en desplazarse entre un supervisor SMTP y su buzón de destino.
$user*(ImapUser)	El nombre de usuario (nombre de cuenta) utilizado por el supervisor para iniciar la sesión en el servidor IMAP4.

Mensaje de estado

El supervisor POP3 proporciona mensajes de estado en el atributo `ResultMessage` cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado de POP3.

Tabla 92. Mensajes de estado del supervisor POP3

Mensaje	Descripción
`Message successfully downloaded` (Mensaje descargado correctamente)	La solicitud POP3 se ha realizado correctamente.
`Downloaded` *x* `messages` (*x* mensajes descargados)	Indica cuántos mensajes se han descargado del buzón.
`Timed out waiting to read/write` (Tiempo de espera superado al esperar lectura/escritura)	Se ha establecido una conexión de datos con el servidor, pero ha dejado de responder.
`Connection closed by foreign host` (Conexión cerrada por host foráneo)	El host remoto ha cerrado la conexión antes de lo que esperaba el supervisor.
`Connection failed` (Error de conexión)	El supervisor no ha podido conectarse al servidor. Consulte el archivo de registro si desea más información.
`APOP not supported by the server` (APOP no soportada por el servidor)	El servidor no admite el método de autenticación APOP. Use en su lugar el tipo de autenticación estándar.
`APOP service not available` (Servicio APOP no disponible)	El servidor no admite la implementación del servidor APOP. Use en su lugar el tipo de autenticación estándar.
`Server does not support STLS capability` (El servidor admite la función STLS)	El servidor no da soporte a STARTTLS. Use un tipo de seguridad distinto.

Propiedades

Las propiedades específicas del supervisor POP3 se describen en la tabla siguiente.

Tabla 93. Propiedades y opciones de la línea de mandatos del supervisor POP3

Nombre de propiedad	Parámetro de propiedad	Descripción
`SSLCertificate File`	serie	La vía de acceso y el nombre de archivo del archivo de certificado digital utilizado si no se especifica ningún certificado de forma explícita para un elemento POP3 durante su creación. Si la vía de acceso no es absoluta, el supervisor lo interpreta como relativo al directorio de trabajo (`$ISHOME/platform/`*`arch`*`/bin`).
`SSLCipherSuite`	serie	La suite de cifrado que se utiliza para las operaciones SSL. Valor predeterminado: `RC4:3DES:DES:+EXP`. Consulte Suites de cifrado para obtener una descripción de los valores posibles.

Tabla 93. Propiedades y opciones de la línea de mandatos del supervisor POP3 (continuación)		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
SSLDisableTLS	entero	Inhabilita TLSv1 para el soporte de legado. Valor predeterminado: 0 - TLSv1 está habilitado. Establézcalo en 1 para inhabilitar TLSv1.
SSLKeyFile	serie	El archivo que contiene la clave privada SSL.
SSLKeyPassword	serie	La contraseña utilizada para cifrar la clave privada SSL.

Suites de cifrado

La propiedad SSLCipherSuite especifica el conjunto de cifrado que utiliza el supervisor POP3. Para más información sobre valores SSL, consulte "Establecimiento de SSL en Internet Service Monitoring" en la página 454.

Supervisor RADIUS

El Servicio de usuario de marcación de autenticación remota (RADIUS) proporciona autenticación para el acceso remoto a los servicios. El supervisor RADIUS simula un sistema de cliente que accede a un servicio RADIUS y devuelve datos sobre el rendimiento del servicio.

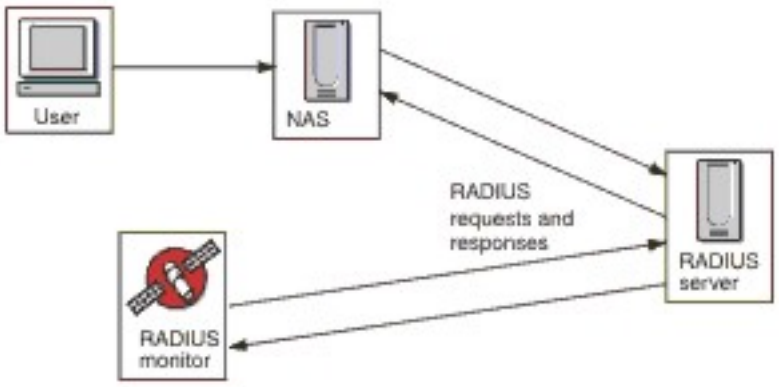
En la tabla siguiente se enumeran los archivos de supervisor RADIUS.

Tabla 94. Archivos del supervisor RADIUS	
Archivos de supervisor	**Nombre y ubicación**
Archivo ejecutable de supervisor	nco_m_radius
Archivo de propiedades	$ISHOME/etc/props/radius.props
Archivo de reglas	$ISHOME/etc/rules/radius.rules
Archivo de registro	$ISHOME/log/http.log

Directrices para configurar el supervisor Radius

El supervisor RADIUS simula el funcionamiento de un servidor NAS (Network Access Server) mediante el envío de solicitudes a un servidor RADIUS.

El supervisor RADIUS utiliza UDP para enviar solicitudes al servidor RADIUS y, a continuación, genera sucesos que contienen los resultados de dichas solicitudes y datos sobre el rendimiento del servidor. La imagen siguiente muestra el funcionamiento del supervisor.



El supervisor puede probar tanto la operación de autenticación como la de contabilidad de los servidores RADIUS:

- Solicitudes de acceso utilizando el Procedimiento de autenticación de contraseña (PAP)
- Solicitudes de acceso utilizando el Protocolo de autenticación por desafío mutuo (CHAP)
- Solicitudes de contabilidad: Start, Stop, Accounting On y Accounting Off

Propiedades

Las opciones de propiedades específicas para el supervisor RADIUS se describen en la tabla siguiente.

Tabla 95. Opciones de propiedades del supervisor RADIUS

Nombre de propiedad	Parámetro de propiedad	Descripción
`FramedServiceRequest`	`0`|`1`	Cuando esta propiedad se configura en `1`, el supervisor selecciona el tipo de servicio Framed configurado en las solicitudes de acceso. `0` - inhabilitado `1` - habilitado

Configuración de pruebas de servicio de supervisor Radius

Utilice los parámetros de configuración del supervisor RADIUS para definir pruebas de servicios.

En la tabla siguiente se describen las configuraciones del supervisor Radius:

Tabla 96. Configuración del supervisor RADIUS

Campo	Descripción
server	Dirección IP del servidor RADIUS.
sharedsecret	Secreto compartido que se utiliza para autenticar el supervisor.
username	Nombre de usuario proporcionado por el supervisor para autenticarse en el servidor RADIUS.
password	Contraseña proporcionada por el supervisor para autenticarse en el servidor RADIUS.
description	Campo de texto para proporcionar información descriptiva sobre el elemento.

Tabla 96. Configuración del supervisor RADIUS (continuación)	
Campo	**Descripción**
requesttype	Especifica el tipo de solicitud enviada al servidor RADIUS: • `Authenticate (CHAP)` • `Authenticate (PAP)` • `Accounting` Valor predeterminado: `Authenticate (CHAP)`
port	Puerto que se utiliza para conectar al servidor RADIUS. Valor predeterminado: 1812
localip	Especifica la dirección IP de la interfaz de red en el sistema host al que se enlaza el supervisor cuando realizar la prueba. Si se configura la propiedad `IpAddress` del supervisor, sustituye el valor de este campo.
loginhost	Establece el valor del atributo `Login-IP-Host` en la solicitud de acceso.
calledstation	Establece el valor del atributo `Called-Station-Id` en la solicitud de acceso.
callingstation	Establece el valor del atributo `Calling-Station-Id` en la solicitud de acceso.
accountsessionid	Establece el valor del atributo `Acct-Session-Id` en paquetes de solicitud de contabilidad enviados al servidor de contabilidad **Nota:** Este campo es aplicable sólo al tipo de solicitud `Accounting`.
accountstatustype	Establece el valor del atributo `Acct-Status-Type` en paquetes de solicitud de contabilidad enviados al servidor de contabilidad: • `Start` • `Stop` • `Accounting On` • `Accounting Off` **Nota:** este campo es aplicable sólo al tipo de solicitud `Accounting`. Valor predeterminado: `Start`
accountsessiontime	Establece el valor del atributo `Acct-Session-Time` (en segundos) en paquetes de solicitud de contabilidad enviados al servidor de contabilidad **Nota:** este campo es aplicable sólo al tipo de solicitud `Accounting`.
nasip	El atributo `NAS-IP-Address` enviado por el supervisor RADIUS como parte de un paquete de Solicitud de acceso.
nasport	El atributo `NAS-Port` enviado por el supervisor RADIUS como parte de un paquete de solicitud de acceso.

Tabla 96. Configuración del supervisor RADIUS (continuación)	
Campo	**Descripción**
timeout	Tiempo de espera, en segundos, para que responda el servidor. Valor predeterminado: `10`
retries	Número de veces para reintentar conectarse al servidor RADIUS si hay un problema. Valor predeterminado: `0`
poll	Tiempo, en segundos, entre cada sondeo. Valor predeterminado: `300`
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: `0`
retestinterval	Tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: `10`

Clasificación de nivel de servicio

Las clasificaciones del nivel de servicio definen las reglas para determinar el nivel de servicio suministrado por el servicio RADIUS.

Las opciones de clasificación del nivel de servicio disponibles para el supervisor RADIUS son estas:

```
totalTime
lookupTime
responseTime
message
```

En las clasificaciones del nivel de servicio:

- Especifique más clasificaciones de nivel de servicio entrando manualmente el nombre del elemento supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección Elementos de supervisor.
- `message` puede ser cualquier mensaje que se reenvíe en el elemento `$message` al servidor IBM Application Performance Management si se utiliza en cualquier widget. Para obtener una lista de valores posibles, consulte Mensajes de estado.
- El operando es una serie o un número positivo.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor RADIUS genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio RADIUS.

En la tabla siguiente se describen los elementos adicionales para el supervisor RADIUS.

Tabla 97. Elementos de supervisor de RADIUS	
Elemento	**Descripción**
`$accountSessionId`	Identificador exclusivo utilizado para correlacionar los registros de inicio y de detención.

Tabla 97. Elementos de supervisor de RADIUS (continuación)	
Elemento	**Descripción**
$accountSessionTime	Cuando accountStatusType se establece en Stop, este campo muestra la cantidad de tiempo que el usuario recibe el servicio, en segundos.
$accountStatusType	Indica si es el inicio del servicio del usuario (start) o el final (stop).
$calledStationId	El supervisor RADIUS envía calledStationId como parte de un paquete de solicitud de acceso. Se utiliza si el servidor RADIUS lo necesita y no se utiliza si se emplea callingStationId.
$callingStationId	El supervisor RADIUS envía callingStationId como parte de un paquete de solicitud de acceso. Se utiliza si el servidor RADIUS lo necesita y no se utiliza si se emplea calledStationId.
$localIP	La dirección IP local configurada para ser utilizada por el supervisor. Puede estar en blanco en un sistema con una sola interfaz.
$loginIPHost* (LoginIpHost)	El supervisor RADIUS envía loginIPHost como parte de un paquete de solicitud de acceso. Es posible que lo necesiten los servidores que se están supervisando.
$lookupTime* (LookupTime)	El tiempo que se tarda en obtener la dirección IP del servidor de host.
$nasPort* (NasPort)	El parámetro NAS Port enviado por el supervisor RADIUS como parte de un paquete de solicitud de acceso. Valor predeterminado: 0.
$password	Contraseña utilizada para autenticar el supervisor.
$port* (Port)	Puerto en que se supervisa el servicio.
$requestType	Indica el tipo de solicitud que se selecciona para el elemento, PAP, CHAP o Accounting.
$responseTime	El tiempo transcurrido desde que se envía una solicitud al servidor RADIUS y se recibe una respuesta del mismo.
$retries	Número máximo de reintentos.
$secret	Contraseña secreta compartida tomada del archivo de configuración.
$username* (RadiusUser)	Nombre de usuario utilizado para autenticar el supervisor.

Mensajes de estado

El supervisor RADIUS proporciona mensajes de estado en el atributo ResultMessage cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado del supervisor RADIUS.

Tabla 98. Mensajes de estado del supervisor RADIUS	
Mensaje	**Descripción**
`CHAP authentication - Access granted` (Autenticación CHAP: acceso concedido)	El supervisor se ha autenticado (utilizando CHAP). Sólo se devuelve si se ha utilizado el tipo de solicitud CHAP.
`PAP authentication - Access granted` (Autenticación PAP: acceso concedido)	El supervisor se ha autenticado (utilizando PAP). Sólo se devuelve si se ha utilizado el tipo de solicitud PAP.
`Accounting response received` (Respuesta de contabilidad recibida)	Se ha recibido una respuesta de contabilidad del servidor. La transacción ha continuado.
`Connection failed` (Error de conexión)	El nombre de servidor especificado no es válido.
`Failed to send request to RADIUS server` (No se ha podido enviar solicitudes al servidor RADIUS)	Es posible que no se pueda grabar el paquete UDP en la red. No hay más información sobre errores disponible.
`No response from server` (No hay respuesta del servidor)	El servidor RADIUS no responde.
`Incorrect identifier returned` (Se ha devuelto un identificador incorrecto)	Ha habido una respuesta del servidor a una solicitud que no se ha enviado desde el supervisor.
`Invalid response authenticator` (Autenticador de respuesta no válido)	La respuesta contenía una autorización inesperada. Puede haberla causado un secreto compartido o una contraseña incorrectos.
`Unrecognized response` (Respuesta no reconocida)	El servidor no ha reconocido el paquete que se ha enviado.
`PAP authentication - Access denied` (Autenticación PAP: acceso denegado)	El supervisor no se ha autenticado (utilizando PAP).
`CHAP authentication - Access denied` (Autenticación CHAP: acceso denegado)	El supervisor no se ha autenticado (utilizando CHAP).

Supervisor RPING

El supervisor RPING prueba la disponibilidad de dispositivos de red haciendo ping en ellos de forma remota desde un direccionador. Proporciona datos de rendimiento de tiempo de ida y vuelta máximo, mínimo y promedio.

El supervisor admite los direccionadores Cisco y Juniper así como los direccionadores compatibles con RFC2925.

En la tabla siguiente se listan los archivos de supervisor de RPING.

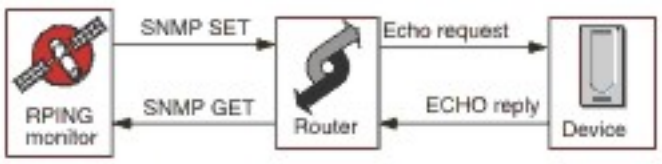
Tabla 99. Archivos del supervisor RPING	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_rping`
Archivo de propiedades	`$ISHOME/etc/ims/props/rping.props`
Archivo de reglas	`$ISHOME/etc/ims/rules/rping.rules`
Archivo de registro	`$ISHOME/log/rping.log`
Archivos de script	`$ISHOME/scripts/rping/cisco.s` (script SNMP para direccionadores Cisco) `$ISHOME/scripts/rping/juniper.s` (script SNMP para direccionadores Juniper) `$ISHOME/scripts/rping/rfc2925.s` (script SNMP para direccionadores compatibles con RFC2925)

Directrices para configurar el supervisor RPING

El supervisor RPING adquiere datos configurando el direccionador para que haga ping en un dispositivo de red, y luego sondeando de forma periódica para obtener los resultados de los pings.

El supervisor configura las pruebas de ping utilizando un mandato SET de SNMP para crear una fila de control en el MIB de ping del direccionador y, a continuación, recupera los datos de ping del MIB utilizando mandatos GET de SNMP. Toda la comunicación con el direccionador se realiza a través de SNMP.

La imagen siguiente muestra un ejemplo de los mensajes que se intercambian entre el supervisor y el dispositivo de red.



Habilitación de solicitud ping remota en direccionadores Cisco

De forma predeterminada, las solicitudes SNMP de ping remotos en los direccionadores Cisco están inhabilitadas. Sin embargo, para que el supervisor RPING realice una solicitud SNMP SET y empiece a emitir pings, esta solicitud debe estar habilitada.

Para habilitar la solicitud, inicie sesión en el direccionador Cisco y especifique los mandatos siguientes:

```
enable
config terminal
snmp-server community serie_comunidad rw
write mem
logout
```

La serie de comunidad configurada en el direccionador debe coincidir con la serie que se especifica en el campo de serie de comunidad de los elementos de perfil RPING que se crean para dicho direccionador. La línea write mem garantiza que los valores se guarden cuando se reinicia el direccionador.

Habilitación de solicitud de ping remota en direccionadores Juniper

De forma predeterminada, las solicitudes de SNMP de ping remoto en direccionadores Juniper están inhabilitadas. Para que el supervisor RPING funcione utilizando un direccionador Juniper, debe habilitar las solicitudes SNMP.

Para habilitar la solicitud SNMP en el direccionador, asegúrese de que la sección SNMP de la configuración JUNOS coincide:

```
[edit snmp]
view ping-mib-view {
  oid .1.3.6.1.2.1.80 include; # pingMIB
  oid jnxPingMIB include; # jnxPingMIB
}
community serie_comunidad {
  authorization read-write;
  view ping-mib-view;
}
```

La serie de comunidad configurada en el direccionador debe coincidir con la serie que se especifica en el campo de serie de comunidad de los elementos de perfil RPING que se configuran para dicho direccionador.

Propiedades

Las opciones de propiedades específicas para el supervisor RPING se describen en la tabla siguiente.

Tabla 100. Opciones de propiedades de RPING

Nombre de propiedad	Parámetro de propiedad	Descripción
MibDir	serie	El directorio que contiene los archivos MIB utilizados por el supervisor. Valor predeterminado: `$ISHOME/mibs`.

Configuración de pruebas de servicios del supervisor RPING

Utilice los parámetros de configuración del supervisor RPING para definir pruebas de servicios.

Tabla 101. Configuración del supervisor RPING

Campo	Descripción
server	Nombre o dirección IP del direccionador. Por ejemplo, `rt1.mycompany.com`.
routertype	El tipo de direccionador: • CISCO • Juniper • RFC2925
host	Nombre o dirección IP del servidor al que se desea que el direccionador haga ping.
communitystring	Especifica la serie de comunidad SNMP que se utiliza para comunicarse con el direccionador. Por ejemplo, `server1.mycompany.com`.
description	Campo de texto para proporcionar información descriptiva sobre el elemento. Por ejemplo, `Supervisor RPING`.

Tabla 101. Configuración del supervisor RPING (continuación)	
Campo	**Descripción**
vpn	Nombre opcional de una VPN que se va a utilizar para el envío de pings. El direccionador utiliza la VPN especificada en lugar de la ruta predeterminada configurada.
version	Versión de SNMP que se va a utilizar: 1 - SNMPv1 2 - SNMPv2c 3 - SNMPv3 Valor predeterminado: 2
numberofpings	Número de pings que se va a enviar. Valor predeterminado: 5
packetsize	Tamaño de los paquetes que se van a enviar, en bytes. Valor predeterminado: 64
packettimeout	Tiempo que se debe esperar entre pings en segundos. Valor predeterminado: 500
securityname†	Nombre de usuario para la sesión SNMP.
authenticationphrase†	Contraseña de autenticación para el usuario.
privacyphrase†	Contraseña de privacidad para el usuario.
authenticationprotocol†	Protocolo que se debe utilizar para autenticar el usuario: • MD5 • SHA1 Valor predeterminado: MD5
privacyprotocol†	Protocolo que se debe utilizar para cifrar la sesión. Valor predeterminado: DES
timeout	El tiempo, en segundos, entre cada sondeo. Valor predeterminado: 10
retries	Número de veces que el supervisor vuelve a intentar contactar con el servidor. Valor predeterminado: 3
poll	Tiempo que se debe esperar entre pings en segundos. Valor predeterminado: 300
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: 0

Tabla 101. Configuración del supervisor RPING (continuación)	
Campo	**Descripción**
retestinterval	Tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: 10
† Sólo aplicable a SNMPv3.	

Clasificación de nivel de servicio

Las clasificaciones del nivel de servicio definen las reglas para determinar el nivel de servicio que se suministra a través de RPING.

Las opciones de clasificación del nivel de servicio disponibles para el supervisor RPING son estas:

```
totalTime
lookupTime
numPacketSent
numPacketsRecv
maxRTT
minRTT
averageRTT
respondPercent
message
```

En las clasificaciones del nivel de servicio:

- Especifique más clasificaciones de nivel de servicio entrando manualmente el nombre del elemento supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección Elementos de supervisor.
- `message` puede ser cualquier mensaje que se reenvíe en el elemento **`$message`** al servidor IBM Application Performance Management si se utiliza en cualquier widget. Para obtener una lista de valores posibles, consulte Mensajes de estado.
- El operando es una serie o un número positivo.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor RPING genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio RPING.

En la tabla siguiente se indican los elementos adicionales para el supervisor RPING.

Tabla 102. Elementos del supervisor RPING	
Elemento	**Descripción**
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.
(AverageRTT)	Tiempo medio de ida y vuelta en segundos.
$community	Serie de comunidad SNMP para el direccionador.
$communityString	Serie de comunidad SNMP que se utiliza para comunicarse con el direccionador.
(MaxRTT)	Tiempo máximo de ida y vuelta en segundos.
(MinRTT)	Tiempo mínimo de ida y vuelta en segundos.
$numPacketSent	Número de paquetes enviados por el supervisor.

Tabla 102. Elementos del supervisor RPING (continuación)	
Elemento	**Descripción**
$numPings	Número de pings enviados, especificado cuando se añadió el elemento RPING.
$packetSize	Tamaño de paquetes por enviar.
$packetTimeout	Tiempo de espera entre cada envío de paquetes.
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.
$remoteHost* (RemoteHost)	Nombre o dirección IP del servidor al que se desea que el direccionador haga ping.
(RespondPercent)	Porcentaje de pings enviados para los que ha habido una respuesta.
$routerMan* (RouterName)	Tipo de direccionador seleccionado cuando se añadió el elemento RPING: • CISCO • Juniper • RFC2925
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
(SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
(SourceRouter)	Nombre o dirección IP del direccionador.
$timeout	Número de segundos en los que debe responder el servidor. Se toma del archivo de configuración.
$vpn* (Vpn)	Nombre de la VPN indicada en el campo **vpn** del elemento de perfil RPING.

Mensajes de estado

El supervisor RPING proporciona mensajes de estado en el atributo **ResultMessage** cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado de RPING.

Tabla 103. Mensajes de estado de supervisor RPING	
Mensaje	**Descripción**
`Got Response` (Respuesta recibida)	El supervisor ha recibido una respuesta del dispositivo Cisco.
`Error in packet - exiting thread` (Error en el paquete - saliendo de la hebra)	Se ha producido un error en uno de los paquetes.

Tabla 103. Mensajes de estado de supervisor RPING (continuación)	
Mensaje	**Descripción**
`Timed out while trying initial sets` (Tiempo de espera excedido en los intentos iniciales)	No se ha recibido ninguna respuesta del direccionador cuando se ha intentado crear el campo `rowEntry`.
`Internal Error` (Error interno)	Error en el direccionador.
`Host poll did not finish` (Sondeo de host no finalizado)	El dispositivo de red no ha finalizado los pings.
`Response Failed` (Respuesta fallida) `Operation Failed` (Operación fallida)	El direccionador no ha podido hacer ping en el dispositivo de red.
`Timed out on Get requests` (Tiempo de espera excedido en las solicitudes Get)	El supervisor ha agotado el tiempo de espera cuando el usuario intentaba obtener los resultados del direccionador.

Supervisor RTSP

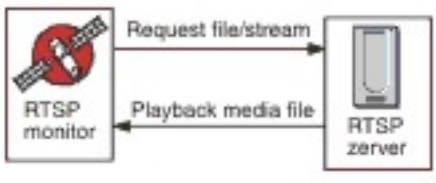
El supervisor Real Time Streaming Protocol (RTSP) prueba la reproducción en streaming de sonido e imagen en servidores de transmisión continua. Recopila información sobre los archivos multimedia e inicia la reproducción de transmisión continua, la pausa y el final de una sesión de transmisión continua.

En la tabla siguiente se listan los archivos del supervisor RTSP.

Tabla 104. Archivos del supervisor RTSP	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_rtsp`
Archivo de propiedades	`$ISHOME/etc/props/rtsp.props`
Archivo de reglas	`$ISHOME/etc/rules/rtsp.rules`
Archivo de registro	`$ISHOME/log/rtsp.log`

Directrices para configurar el supervisor RTSP

El supervisor RTSP se conecta con el servidor de transmisión tanto en la modalidad DESCRIBE como en la modalidad PLAY. El supervisor descarga información o estadísticas suministradas por servidores RTSP reales como Darwin.



Modalidad DESCRIBE

En la modalidad DESCRIBE, el supervisor RTSP se conecta al servidor de transmisión continua y solicita información acerca de los archivos y secuencias de audio y vídeo.

El servidor devuelve un código de estado en el que un valor de 200 indica un archivo que se puede descargar, y donde otros valores indican por qué no se puede reproducir el archivo solicitado.

Sin embargo, las estadísticas relacionadas con la reproducción no se notifican en esta modalidad; puede probarse la función básica de los servidores que dan soporte a RTSP.

Modalidad PLAY

En la modalidad PLAY, el supervisor RTSP se conecta al servidor de transmisión continua del mismo modo que en la modalidad DESCRIBE y, a continuación, transmite el archivo para suministrar estadísticas sobre las descargas solicitadas.

Propiedades

Las opciones de propiedades específicas para el supervisor RTSP se describen en la tabla siguiente.

Tabla 105. Opciones de propiedades del supervisor RTSP

Nombre de propiedad	Parámetro de propiedad	Descripción
StreamingSocket BufferSize	entero	Tamaño del almacenamiento intermedio de socket de modalidad continua, con un rango de entre 8 y 64 KB. Valor predeterminado: 8

Configuración de pruebas de servicios del supervisor RTSP

Utilice los parámetros de configuración del supervisor RTSP para definir pruebas de servicios.

En la tabla siguiente se listan las configuraciones del supervisor RTSP:

Tabla 106. Configuración del supervisor RTSP

Campo	Descripción
server	Sistema de destino que ejecuta el servidor de modalidad continua. Por ejemplo, `rtsp.mymusic.com`.
remotefile	Archivo que se descarga. Por ejemplo, `singalong.mp3`.
description	Campo de texto que proporciona información descriptiva sobre el elemento. Por ejemplo, `Supervisor RTSP`.
port	Puerto al que se conecta el servidor en el sistema de destino. Valor predeterminado: 554
action	Acción que realiza el servidor en la transmisión: • DESCRIBE • PLAY Valor predeterminado: DESCRIBE
duration	Parte de la transmisión, en segundos, que el servidor reproduce. Valor predeterminado: 5
maxbandwidth	Ancho de banda máximo, en bits por segundo, que se utiliza para la transmisión. Valor predeterminado: 1500000

Tabla 106. Configuración del supervisor RTSP (continuación)	
Campo	**Descripción**
timeout	Tiempo de espera, en segundos, para que responda el servidor RTSP. Valor predeterminado: 10
poll	Tiempo, en segundos, entre cada sondeo. Valor predeterminado: 300
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: 0
retestinterval	Tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: 10

Clasificaciones de nivel de servicio

Las clasificaciones del nivel de servicio definen las reglas para determinar el nivel de servicio que se suministra a través de RTSP.

Las opciones de clasificación del nivel de servicio disponibles para el supervisor RTSP son estas:

```
totalTime
lookupTime
connectTime
responseTime
sdpDownloadTime
playbackTime
estatus
percentPacketsLost
message
```

En las clasificaciones del nivel de servicio:

- Especifique más clasificaciones de nivel de servicio entrando manualmente el nombre del elemento supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección de elementos de supervisor.
- `message` puede ser cualquier mensaje que se reenvíe en el elemento **`$message`** al servidor IBM Application Performance Management si se utiliza en cualquier widget. Para obtener una lista de valores posibles, consulte Mensajes de estado.
- El operando es una serie o un número positivo.
- Un código de estado 200 indica éxito. Consulte el protocolo RTSP para ver otros códigos de estado devueltos por la operación.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor RTSP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio RTSP.

En la tabla siguiente se describen los elementos adicionales para el supervisor RTSP.

Tabla 107. Elementos del supervisor RTSP	
Elemento	**Descripción**
$action	Acción que lleva a cabo el supervisor.

Tabla 107. Elementos del supervisor RTSP (continuación)	
Elemento	**Descripción**
$averageBandwidth	Ancho de banda total medio, en bits.
$bytesReceived	Número total de bytes recibidos.
$connectTime* (ConnectTime)	Tiempo que se tarda en establecer una conexión con el servidor de destino.
$describeStageStatus	Código de estado para una fase de la conversación RTSP.
$filename	Nombre del archivo multimedia.
$lookupTime* (LookupTime)	Tiempo que se tarda en obtener la dirección IP del servidor de host.
$maxBandwidth	Ancho de banda máximo utilizando la interfaz de configuración.
$mediaResponseTime	Tiempo que tarda el servidor en iniciar la transmisión del archivo solicitado.
$numberOfStreams	Número de secuencias incluidas en los medios.
$percentPacketsLost	Porcentaje de paquetes perdidos.
$playbackTime* (PlaybackTime)	Tiempo que representa la suma de setupResponseTime y mediaResponseTime.
$playStageStatus	Código de estado para una fase de la conversación RTSP.
$port	Puerto utilizado para acceder al servidor del supervisor.
$responseTime* (ResponseTime)	Tiempo transcurrido desde que se establece la conexión hasta que se recibe el primer byte de datos.
$sdpDownloadTime* (SdpDownloadTimed)	Tiempo que se tarda en descargar datos sobre el archivo multimedia.
$setupResponseTime	Tiempo que representa parte de playbackTime. **Nota:** El elemento sólo se genera cuando el supervisor RTSP funciona en modalidad de reproducción (PLAY).
$setupStageStatus	Código de estado para una fase de la conversación RTSP.
$status	Código de estado devuelto por el servidor RTSP.
$streamingTime	Tiempo que tarda el servidor en completar la transmisión del archivo solicitado.
$streamLength	Longitud de la secuencia más larga del archivo multimedia.

Tabla 107. Elementos del supervisor RTSP (continuación)	
Elemento	**Descripción**
$teardownStageStatus	Código de estado para una fase de la conversación RTSP.
$totalBandwidthRequired	Ancho de banda total en kilobits por segundo
$totalPacketsLost	Número total de paquetes perdidos.
$totalPacketsReceived	Número de paquetes recibidos.

Mensajes de estado

El supervisor RTSP proporciona mensajes de estado en el atributo **`ResultMessage`** cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

Tabla 108. Mensajes de estado de supervisor RTSP	
Mensaje	**Descripción**
OK (CORRECTO)	La solicitud se ha realizado correctamente.
`Connection failed` (Error de conexión)	El supervisor no ha podido conectarse al servidor. Para obtener más información, consulte el archivo de registro.
`Connection closed by foreign host` (Conexión cerrada por host foráneo)	La conexión con el servidor RTSP se ha interrumpido.
`Timed out waiting to read/write` (Tiempo de espera superado al esperar lectura/escritura)	Una conexión de datos con el servidor RTSP se ha establecido, pero se ha producido un problema.
`Play failed - no streams` (Ha fallado la reproducción: no hay secuencias)	El supervisor ha recibido una respuesta, pero no había ningún archivo de sonido o imagen para su reproducción.
`select() failed on RTSP socket (PLAY stage)` select() ha fallado en el socket RTSP (fase de reproducción)	El socket se ha cerrado desde el servidor remoto, o se ha superado el tiempo de espera esperando una respuesta.
`RTSP Server response not in expected format` (La respuesta de servidor RTSP no tiene el formato esperado)	La respuesta del servidor estaba en un formato que el supervisor no soporta.
`Redirection requested by server not supported by client` (La redirección solicitada por el servidor no soportada por el cliente)	La respuesta del servidor no es soportada por el cliente.
`Server cannot fulfill client request` (El servidor no puede completar la solicitud del cliente)	La solicitud ha fallado y no hay más información disponible.

Tabla 108. Mensajes de estado de supervisor RTSP (continuación)	
Mensaje	**Descripción**
`Server Error` (Error del servidor)	Ha habido un problema con el servidor y la solicitud ha fallado. El servidor ha devuelto un código `500` o superior. Para obtener más información, consulte el protocolo RTSP (RFC 2326).

Tabla 108. Mensajes de estado de supervisor RTSP (continuación)	
Mensaje	**Descripción**
`RTSP response header CSeq doesn't match request CSeq` (El valor de CSeq de la cabecera de respuesta RTSP no coincide con el valor de CSeq de la solicitud)	El servidor RTSP está mal configurado y no funciona correctamente.
`Corrupted RTSP server response` (Respuesta de servidor RTSP dañada)	
`Corrupted session description` (Descripción de sesión dañada)	
`RTSP SETUP response CSeq doesn't match request CSeq` (El valor de CSeq de la respuesta de RTSP SETUP no coincide con el valor de CSeq de la solicitud)	
`RTSP SETUP response, incomplete Session string` (Respuesta de RTSP SETUP, cadena de sesión incompleta)	
`RTSP SETUP response, Session ID has changed within the same session` (Respuesta de RTSP SETUP, el ID de sesión ha cambiado en la misma sesión)	
`RTSP SETUP response does not contain server ports to connect to` (La respuesta RTSP SETUP no contiene puertos de servidor con los que conectarse)	
`RTSP SETUP response does not contain server port pair to connect to` (La respuesta RTSP SETUP no contiene un par de puertos de servidor con los que conectarse)	
`RTSP PLAY response CSeq doesn't match request CSeq` (El valor de CSeq de la respuesta de RTSP SETUP no coincide con el valor Cseq de la solicitud)	
`RTSP PLAY response, incomplete Session string` (Respuesta de RTSP PLAY, cadena de sesión incompleta)	
`RTSP PLAY response, Session ID has changed within the same session` (Respuesta de RTSP PLAY, el ID de sesión ha cambiado en la misma sesión)	
`RTSP PLAY response, incomplete RTP-Info string` (Respuesta de RTSP PLAY, cadena de RTF-Info incompleta)	
`RTSP PLAY response does not valid RTP seqnum in RTP-Info response` (La respuesta de RTSP PLAY no es un número de secuencia RTP válido en la respuesta de RTP-	

Supervisor SAA

Service Assurance Agent (SAA) de Cisco es un agente de supervisión de rendimiento para productos Cisco para IOS versión 12.2(2) y superiores.

El supervisor SAA utiliza el recurso Service Assurance Agent de Cisco para probar diversas temporizaciones entre los direccionadores de Cisco.

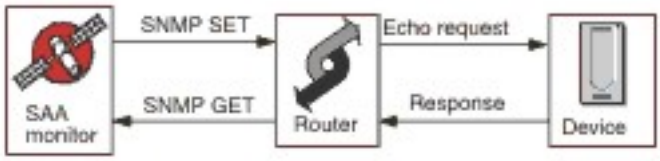
Tabla 109. Resumen del supervisor SAA

Archivos de supervisor	**Nombre o ubicación**
Nombre de ejecutable	`nco_m_saa`
Archivo de propiedades	`$ISHOME/etc/props/saa.props`
Archivo de reglas	`$ISHOME/etc/rules/saa.rules`
Archivo de registro	`$ISHOME/log/saa.log`
Directorio de scripts	`$ISHOME/scripts/saa/`

Directrices para configurar el supervisor SAA

El supervisor SAA configura el SAA de un direccionador para probar la disponibilidad de otro dispositivo o servicio de red utilizando solicitudes o respuestas de eco temporizadas definidas en la MIB (Management Information Base) del Supervisor de tiempo de respuesta de Cisco. El supervisor utiliza el protocolo simple de gestión de red para comunicarse con Service Assurance Agent.

La imagen siguiente muestra la operación del supervisor SAA.



Operación

l supervisor SAA configura el Service Assurance Agent para que ejecute pruebas de eco, denominadas análisis, en otros dispositivos de red. Puede configurar varios análisis diferentes, y que cada uno utilice un protocolo distinto.

Todos los análisis pueden operar con respecto a cualquier destino habilitado para IP, excepto Jitter, que necesita otro direccionador de respuesta Cisco con posibilidades SAA.

Cada elemento de perfil de supervisor inicia un análisis de Service Assurance Agent en un direccionador en el inicio y con cada sondeo sucesivo, recopila información de resultados y vuelve a planificar el análisis. Si un análisis se detiene de forma inesperada, el supervisor lo reinicia inmediatamente. Cuando las pruebas de análisis se han completado, pasa a estado inactivo hasta el siguiente sondeo de supervisor. En el siguiente sondeo de supervisor, se recopilan los datos de resultado y empieza otro ciclo de prueba. Durante cada sondeo, el supervisor comprueba el estado del análisis. Si el análisis aún se está ejecutando, el supervisor lo detiene y, a continuación, sondea en MIB (Management Information Base) los datos de resultado y la información de error del último ciclo. A continuación, vuelve a planificar el análisis, restablece los datos estadísticos y reactiva el análisis, que se ejecuta desatendido hasta el siguiente sondeo de supervisor.

Para evitar la posibilidad de que haya procesos no controlados en el direccionador, el supervisor inicia análisis con una duración predefinida que se amplía en cada sondeo de supervisor. Si el supervisor termina, continúa ejecutándose hasta que caduca su lapso de vida. A partir de entonces, pasa al estado inactivo hasta que se alcanza un tiempo de antigüedad y el direccionador finaliza el proceso.

No es necesario para IOS y Service Assurance Agent preconfigurados porque el supervisor configura, controla y limpia automáticamente después de los análisis en tiempo de ejecución. Esto incluye la configuración de direccionadores de respuesta que son necesarios para varios tipos de análisis.

Persistencia de los análisis
La propiedad de supervisor ProbePersist controla la persistencia de análisis a lo largo de los sondeos de supervisor. Si la persistencia de análisis no se ha habilitado, los análisis se inician en cada sondeo y finalizan inmediatamente después de producir los resultados de prueba.

Carga del direccionador
En ocasiones, las operaciones de los análisis pueden verse afectadas por la carga del direccionador. La propiedad StatusWait proporciona análisis con la hora para cambiar de un estado a otro antes de que se considere que una operación ha fallado.

Tipos de análisis
Los tipos de análisis disponibles con el supervisor SAA se listan a continuación:

- DHCP
- DLSW
- DNS
- FTP
- Solicitudes Get HTTP
- Eco de ICMP
- Eco de vía de acceso ICMP
- Jitter
- Eco de UDP
- Eco de SNA
- VOIP

Los análisis de eco realizan pruebas basándose en un periodo de tiempo, mientras que los análisis de Jitter, VOIP y HTTP realizan pruebas por operación única.

Propiedades de SAA
Debe establecer las propiedades del supervisor SAA.

En la tabla siguiente se describen las propiedades del supervisor SAA.

Tabla 110. Propiedades del supervisor SAA

Nombre de propiedad	Parámetro de propiedad	Descripción
AgeOut	entero	Número máximo de segundos que un análisis permanece inactivo antes de detenerse. El valor predeterminado es 600.
MibDir	serie	Directorio que se utiliza para los archivos MIB. La vía de acceso predeterminada es `$ISHOME/mibs`.
ProbeLife	entero	Número máximo de segundos que un análisis permanece activo cuando está desatendido. El valor predeterminado es 600.

Tabla 110. Propiedades del supervisor SAA (continuación)		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
ProbePersist	0|1	Los análisis pueden ejecutarse en dos modalidades. Realizan un ciclo de pruebas único por sondeo de supervisor o se inician una vez y se vuelven a planificar en cada sondeo. • 0 indica ciclo de pruebas único • 1 indica volver a planificar en cada sondeo
StatusWait	entero	Número de segundos que un supervisor espera a que un análisis complete cualquier acción antes de fallar.

Configuración de pruebas de servicio de supervisor SAA
Debe configurar parámetros de supervisor SAA para definir pruebas de servicio.

En la tabla siguiente se describen los campos de configuración de supervisor SAA.

Tabla 111. Configuración del supervisor SAA	
Campo	**Descripción**
server	Nombre o dirección IP del direccionador Cisco.
communitystring	Serie de comunidad SNMP para el direccionador.
probetype	Tipo de análisis SAA que se aplica al elemento de perfil.
description	Campo de texto que proporciona información descriptiva sobre el elemento.
Active	Indica si el elemento de perfil está activo.
port	Puerto utilizado para acceder al direccionador. El puerto predeterminado es 161.
version	La versión de SNMP que se va a utilizar: • 1 se utiliza para SNMPv1 • 2 se utiliza para SNMPv2c • 3 se utiliza para SNMPv3 El valor predeterminado es 1.
probeid	Especifica un valor que se utiliza para generar el índice de fila de control de análisis.
securityname†	Nombre de usuario para la sesión SNMP.
authenticationphrase†	Contraseña de autenticación para el usuario.
privacyphrase†	Contraseña de privacidad para el usuario.
authenticationprotocol†	Los protocolos que se utilizan para autenticar los usuarios son los siguientes: • MD5 • SHA1 El valor predeterminado es MD5.
privacyprotocol†	Protocolo que se debe utilizar para cifrar la sesión, que es DES.

Tabla 111. Configuración del supervisor SAA (continuación)	
Campo	**Descripción**
timeout	Tiempo, en segundos, que se debe esperar a que responda el direccionador. El valor predeterminado es 5.
retries	Número de veces que el supervisor debe reintentar contactar con el direccionador antes de efectuar la salida. El valor predeterminado es 0.
poll	Tiempo, en segundos, entre cada sondeo. El valor predeterminado es 300
failureretests	Número de veces que se deben volver a realizar pruebas antes de indicar una anomalía. El valor predeterminado es 0.
retestinterval	Tiempo de espera, en segundos, entre cada repetición de prueba tras una anomalía. El valor predeterminado es 10.

Nota: † Sólo aplicable a SNMPv3.

Configuración del tipo de análisis

La configuración de análisis es diferente para cada tipo de análisis y el agente de Internet Service Monitoring proporciona un conjunto de campos de configuración específicos de cada tipo. Para crear un elemento de perfil, seleccione un tipo de análisis y, a continuación, proporcione la configuración apropiada para dicho tipo. Para obtener información sobre elementos de configuración individuales, consulte el documento del MIB de Cisco Response Time Monitor.

Clasificación de nivel de servicio

La clasificación de nivel de servicio define las reglas para determinar el nivel de servicio proporcionado por un dispositivo de red.

Las opciones de clasificación de nivel de servicio disponibles para el supervisor SAA son las siguientes:

```
totalTime
errTotal
numRTT
minRTT
maxRTT
avgRTT
minPosJitterSD
maxPosJitterSD
minNegJitterSD
maxNegJitterSD
minPosJitterDS
maxPosJitterDS
minNegJitterDS
maxNegJitterDS
packetLossSD
packetLossDS
packetOutOfSequence
packetMIA
packetLateArrival
minDelaySD
maxDelaySD
minDelayDS
maxDelayDS
avgPosJitterSD
avgPosJitterDS
```

```
avgNegjitterSD
avgNegJitterDS
avgDelaySD
avgDelayDS
devPosJitterSD
devPosJitterDS
devNegJitterSD
devNegJitterDS
devDelaySD
devDelayDS
MOS
ICPIF
mMinRTT
httpRTT
dnsRTT
tcpConnectRTT
transactionRTT
message
```

En las clasificaciones del nivel de servicio:

- Especifique más clasificaciones de nivel de servicio entrando manualmente el nombre del elemento supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección Elementos de supervisor.
- `message` puede ser cualquier mensaje que se reenvíe en el elemento **$message** al servidor IBM Application Performance Management si se utiliza en cualquier widget. Para ver una lista de valores posibles, consulte "Mensajes de estado" en la página 420.
- El operando es una serie o un número positivo.

Elementos de supervisor
Además de los resultados de prueba comunes a todos los elementos, el supervisor SAA genera un conjunto de resultados de prueba que contiene datos específicos del tipo de análisis que se está utilizando.

Análisis de DHCP
Los análisis de DHCP generan varios elementos.

En la tabla siguiente se describen los elementos de análisis DHCP.

Tabla 112. Elementos del análisis DHCP

Elemento	**Descripción**
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.
$community	Comunidad utilizada para enviar solicitudes de SNMP al SAA.
$port	Puerto utilizado para conectarse con el SAA.
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.
$probeType	dhcp
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
$snmpVersion (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
(SourceRouter)	Nombre del direccionador utilizado para enviar solicitudes de DHCP.
$totalRTT † (TotalRTT)	Tiempo total de ida y vuelta necesario para obtener una IP del servidor DHCP en segundos.

Nota: † indica que el elemento está disponible para las clasificaciones del nivel de servicio.

Análisis de DLSW
Los análisis de DLSW generan varios elementos.

En la tabla siguiente se describen los elementos de análisis de DLSW.

Tabla 113. Elementos de análisis de DLSW	
Elemento	**Descripción**
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.
$avgRTT* † (AverageRTT)	Tiempo medio de ida y vuelta en segundos.
$community	Comunidad utilizada para enviar solicitudes de SNMP al SAA.
$errTotal* † (ErrorTotal)	Número total de paquetes con errores.
$maxRTT* † (MaximumRTT)	Tiempo máximo de ida y vuelta en segundos.
$minRTT* † (MinimumRTT)	Tiempo mínimo de ida y vuelta en segundos.
$numRTT†	Número de viajes de ida y vuelta correctos.
$port	Puerto utilizado para conectarse con el SAA.
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.
$probeType †	dlsw
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
$snmpVersion (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
(SourceRouter)	Direccionador utilizado para realizar la prueba SAA.
$sumOfRTT (TotalRTT)	Suma de todos los tiempos de ida y vuelta en segundos.
(TargetHost)	Nombre o la dirección IP del host en el que se está ejecutando el SAA de destino.

Nota: † indica que el elemento está disponible para las clasificaciones del nivel de servicio.

Análisis de DNS
Los análisis de DNS generan varios elementos.

En la tabla siguiente se describen los elementos de análisis de DNS.

Tabla 114. Elementos del análisis de DNS	
Elemento	**Descripción**
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.

Tabla 114. Elementos del análisis de DNS (continuación)	
Elemento	**Descripción**
$community	Comunidad utilizada para enviar solicitudes de SNMP al SAA.
$dnsHost (Host)	Host que debe resolverse desde el servidor.
$dnsServer	IP del servidor DNS.
(HostLookup)	Dirección IP del host.
$port	Puerto utilizado para conectarse con el SAA.
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.
$probeType	dns
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
$snmpVersion (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
(SourceRouter)	Nombre del direccionador utilizado para enviar solicitudes de DNS.
$totalRTT † (TotalRTT)	Tiempo total de ida y vuelta para la búsqueda de DNS en segundos.

Nota: † indica que el elemento está disponible para las clasificaciones del nivel de servicio.

Análisis de FTP
Los análisis de FTP generan varios elementos.

En la tabla siguiente se describen los elementos de análisis de FTP.

Tabla 115. Elementos del análisis de FTP	
Elemento	**Descripción**
$activePassive	Tipo de conexión utilizado en esta prueba, ya sea `Active` (Activo) o `Passive` (Pasivo). Valor predeterminado: `Passive`
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.
$community	Comunidad utilizada para enviar solicitudes de SNMP al SAA.
$errorStatus	Serie de resultados que indica el estado de la prueba (desde el objeto MIB `rttMonLatestRttOperSense`).
$ftpFile	Nombre del archivo de prueba recuperado durante la prueba.
$ftpUrl (FtpUrl)	URL utilizado en la prueba de FTP.
$port	Puerto utilizado para conectarse con el SAA.
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.

Tabla 115. Elementos del análisis de FTP (continuación)	
Elemento	**Descripción**
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
$snmpVersion (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
(SourceRouter)	Nombre del direccionador utilizado para enviar solicitudes de FTP.
$totalRTT (TotalRTT)	Tiempo de finalización de la prueba (desde el objeto MIB `rttMonLatestRttOperCompletionTime`) en segundos.

Análisis HTTP-Get
Los análisis de HTTP-Get generan varios elementos.

En la tabla siguiente se describen los elementos de análisis de HTTP-Get.

Tabla 116. Elementos del análisis de HTTP-Get	
Elemento	**Descripción**
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.
$community	Comunidad utilizada para enviar solicitudes de SNMP al SAA.
$dnsRTT † (DnsRTT)	Tiempo de ida y vuelta para realizar la consulta de DNS en segundos.
$httpRTT † (HttpRTT)	Tiempo de ida y vuelta para realizar la operación HTTP en segundos.
(HttpUrl)	URL que se supervisa.
$messageBodyBytes	Tamaño del cuerpo del mensaje recibido.
$numRTT†	Número de viajes de ida y vuelta correctos.
$port	Puerto utilizado para conectarse con el SAA.
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.
$probeType	http-get
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
(SourceRouter)	Nombre del direccionador utilizado para enviar solicitudes de HTTP.
$snmpVersion (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
$targetHost	Nombre del host para el servicio que se va a probar.
$tcpConnectRTT † (TcpConnectRTT)	Tiempo de ida y vuelta para conectar con el servidor HTTP en segundos.

Tabla 116. Elementos del análisis de HTTP-Get (continuación)	
Elemento	**Descripción**
$transactionRTT † (TransactionRTT)	Tiempo de ida y vuelta para descargar el objeto especificado por el URL en segundos.

Nota: † indica que el elemento está disponible para las clasificaciones del nivel de servicio.

Análisis de ICMP-Echo
Los análisis de eco ICMP generan varios elementos.

En la tabla siguiente se describen los elementos de análisis de eco ICMP.

Tabla 117. Elementos del análisis de eco ICMP	
Elemento	**Descripción**
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.
$avgRTT † (AverageRTT)	Tiempo medio de ida y vuelta en segundos.
$community	Comunidad utilizada para enviar solicitudes de SNMP al SAA.
$errBusies	Número de pings que han fallado debido a un ping incompleto anterior.
$errDisconnects	Número de pings que han fallado a través de las desconexiones.
$ErrDrops	Número de pings que han fallado porque un recurso interno no estaba disponible.
$errNoConnects	Número de pings que han fallado porque es posible que no se haya establecido una conexión con el destino.
$errSequences	Número de pings ha fallado porque se ha recibido un ID de secuencia inesperado.
$errTimeouts	Número de pings que han fallado en los tiempos de espera.
$errTotal † (ErrorTotal)	Número total de paquetes con errores.
$errVerifies	Número de pings que ha fallado porque los datos recibidos no eran los mismos que los datos esperados.
$maxRTT † (MaximumRTT)	Tiempo máximo de ida y vuelta en segundos.
$minRTT † (MinimumRTT)	Tiempo mínimo de ida y vuelta en segundos.
$numRTT †	Número de viajes de ida y vuelta correctos.
$port	Puerto utilizado para conectarse con el SAA.
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.

Tabla 117. Elementos del análisis de eco ICMP (continuación)	
Elemento	**Descripción**
$probeType	El tipo de análisis debe ser el siguiente: • icmp-echo • icmp-echo-path • udp-echo
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
$snmpVersion (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
(SourceRouter)	Nombre del direccionador utilizado para enviar solicitudes de ICMP.
$sumOfRTT	Suma de todos los tiempos de ida y vuelta en segundos.
$targetHost (Host)	Nombre de host del servicio que se supervisa.
$tos (Tos)	Tipo del valor del servicio.
$vpn (Vpn)	Nombre de la VPN.

Nota: † indica que el elemento está disponible para las clasificaciones del nivel de servicio.

Análisis de ICMP-Path-Echo
Los análisis de ICMP-Patch-Echo generan varios elementos.

En la tabla siguiente se describen los elementos de análisis ICMP-Patch-Echo.

Tabla 118. Elementos del análisis de ICMP-Path-Echo	
Elemento	**Descripción**
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.
$avgRTT † (AverageRTT)	Tiempo medio de ida y vuelta en segundos.
$community	Comunidad utilizada para enviar solicitudes de SNMP al SAA.
(HopHost*Uno a ocho*)	Del primer al octavo host que visitan utilizando ICMP Echo Path.
$maxRTT † (MaximumRTT)	Tiempo máximo de ida y vuelta en segundos.
$minRTT † (MinimumRTT)	Tiempo mínimo de ida y vuelta en segundos.
$numRTT †	Número de viajes de ida y vuelta correctos.
$port	Puerto utilizado para conectarse con el SAA.

Tabla 118. Elementos del análisis de ICMP-Path-Echo (continuación)	
Elemento	**Descripción**
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.
$probeType	El tipo de análisis es el siguiente: • icmp-echo • icmp-echo-path
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
$snmpVersion (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
(SourceRouter)	Nombre del direccionador utilizado para enviar solicitudes de ICMP.
$sumOfRTT	Suma de todos los tiempos de ida y vuelta en segundos.
$targetHost	Nombre del host para el servicio que se va a probar.
$tos (Tos)	Tipo del valor del servicio.
$vpn (Vpn)	Nombre de la VPN.

Nota: † indica que el elemento está disponible para las clasificaciones del nivel de servicio.

Análisis de Jitter
Los análisis de Jitter generan varios elementos.

En la tabla siguiente se describen los elementos de análisis de Jitter.

Tabla 119. Elementos del análisis de Jitter	
Elemento	**Descripción**
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.
$avgDelayDS†	Retraso medio del destino al origen en segundos.
$avgDelaySD†	Retraso medio del origen al destino en segundos.
$avgNegJitterDS†	Jitter negativo medio del destino al origen en segundos.
$avgNegJitterSD†	Jitter negativo medio del origen al destino en segundos.
$avgPosJitterDS†	Jitter positivo medio del destino al origen en segundos.
$avgPosJitterSD†	Jitter positivo medio del origen al destino en segundos.
$avgRTT † (AverageRTT)	Tiempo medio de ida y vuelta en segundos.
$community	Comunidad utilizada para enviar solicitudes de SNMP al SAA.
$devDelayDS†	Desviación estándar de retraso del destino al origen.
$devDelaySD†	Desviación estándar del retraso del origen al destino.

Tabla 119. Elementos del análisis de Jitter (continuación)	
Elemento	**Descripción**
$devNegJitterDS†	Desviación estándar del Jitter negativo del destino al origen.
$devNegJitterSD†	Desviación estándar del Jitter negativo del origen al destino.
$devPosJitterDS†	Desviación estándar del Jitter positivo del destino al origen.
$devPosJitterSD†	Desviación estándar del Jitter positivo del origen al destino.
$errDescription	Descripción del error.
$errTotal (ErrorTotal)	Número total de paquetes con errores.
$maxDelayDS †	Retraso máximo del destino al origen en segundos.
$maxDelaySD †	Retraso máximo del origen al destino en segundos.
$maxNegJitterDS †	Valor de Jitter negativo máximo del destino al origen en segundos.
$maxNegJitterSD †	Valor de Jitter negativo máximo del origen al destino en segundos.
$maxPosJitterDS †	Valor de Jitter positivo máximo del destino al origen en segundos.
$maxPosJitterSD †	Valor de Jitter positivo máximo del origen al destino en segundos.
$maxRTT † (MaximumRTT)	Tiempo máximo de ida y vuelta en segundos.
$minDelayDS †	Retraso mínimo del destino al origen en segundos.
$minDelaySD †	Retraso mínimo del origen al destino en segundos.
$minNegJitterDS †	Valor de Jitter negativo mínimo del destino al origen en segundos.
$minNegJitterSD †	Valor de Jitter negativo mínimo del origen al destino en segundos.
$minPosJitterDS †	Valor de Jitter positivo mínimo del destino al origen en segundos.
$minPosJitterSD †	Valor de Jitter positivo mínimo del origen al destino en segundos.
$minRTT † (MinimumRTT)	Tiempo mínimo de ida y vuelta en segundos.
$numNegJitterDS	Número de valores de Jitter negativo del destino al origen.
$numNegJitterSD	Número de valores de Jitter negativo del origen al destino.
$numOW	Número de operaciones unidireccionales de retardo.
$numPosJitterDS	Número de valores de Jitter positivos del destino al origen.
$numPosJitterSD	Número de valores de Jitter positivo del origen al destino.
$numRTT †	Número de viajes de ida y vuelta correctos.
$packetLateArrival †	Número de paquetes que llegaron después del tiempo de espera.
$packetLossDS †	Número de paquetes que se pierden del destino al origen.
$packetLossSD †	Número de paquetes que se pierden del origen al destino.

Tabla 119. Elementos del análisis de Jitter (continuación)	
Elemento	**Descripción**
$packetMIA†	Número de paquetes que se pierden donde la dirección es desconocida.
$packetOutOfSequence†	Número de paquetes devueltos que no funcionan.
$port	Puerto utilizado para conectarse con el SAA.
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.
$probeType†	Jitter
(ResponderRouter)	Nombre del direccionador que se utiliza para responder a las solicitudes de Jitter.
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
(SourceRouter)	Nombre del direccionador que se utiliza para enviar las solicitudes de Jitter.
$snmpVersion (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
$sum2DelayDS	Suma de cuadrados de retrasos del destino al origen.
$sum2DelaySD	Suma de cuadrados de retrasos del origen al destino.
$sum2NegJitterDS	Suma de cuadrados de todos los valores de Jitter negativos.
$sum2NegJitterSD	Suma de cuadrados de todos los valores de Jitter negativos.
$sum2PosJitterDS	Suma de cuadrados de todos los valores de Jitter positivos.
$sum2PosJitterSD	Suma de cuadrados de todos los valores de Jitter positivos.
$sum2Rtt†	Suma de cuadrados de los valores de ida y vuelta en segundos.
$sumDelayDS	Suma de retrasos del destino al origen en segundos.
$sumDelaySD	Suma de retrasos del origen al destino en segundos.
$sumNegJitterDS	Suma de todos los valores de Jitter negativos en segundos.
$sumNegJitterSD	Suma de los valores de Jitter negativos en segundos.
$sumPosJitterDS	Suma de todos los valores de Jitter positivos en segundos.
$sumPosJitterSD	Suma de todos los valores de Jitter positivos en segundos.
$sumRTT	Suma de todos los viajes de ida y vuelta en segundos.
$targetHost	Nombre del host para el servicio que se va a probar.
$tos (Tos)	Tipo del valor del servicio.
$vpn (\Vpn)	Nombre de la VPN.

Nota: † indica que el elemento está disponible para las clasificaciones del nivel de servicio.

Análisis SNA-Echo
Los análisis SNA-Echo (SNA-RU-Echo, SNA-LU0-Echo, SNA-LU2-Echo, SNA-LU62-Echo y SNA-LU62Native-Echo) generan los elementos que se listan en la tabla siguiente.

En la tabla siguiente se describen los elementos de análisis JSNA-Echo.

Tabla 120. Elementos de análisis de SNA-Echo	
Elemento	**Descripción**
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.
$avgRTT † (AverageRTT)	Tiempo medio de ida y vuelta en segundos.
$community	Comunidad utilizada para enviar solicitudes de SNMP al SAA.
$errTotal †	Número total de paquetes con errores.
$maxRTT † (MaximumRTT)	Tiempo máximo de ida y vuelta en segundos.
$minRTT † (MinimumRTT)	Tiempo mínimo de ida y vuelta en segundos.
$numRTT†	Número de viajes de ida y vuelta correctos.
$port	Puerto utilizado para conectarse con el SAA.
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.
$probeType (ProbeType)	sna-*nombre*-echo
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
(SourceRouter)	Nombre del direccionador que se utiliza para enviar las solicitudes de SNA.
$snmpVersion (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
$sumOfRTT (TotalRTT)	Suma de todos los tiempos de ida y vuelta en segundos.
(TargetHost)	Destino del host para la solicitud de eco SNA.

Nota: † indica que el elemento está disponible para las clasificaciones del nivel de servicio.

Análisis de UDP-Echo
Los análisis de eco de UDP generan los elementos que se muestran en la tabla siguiente.

En la tabla siguiente se describen los elementos de análisis UDP-Echo.

Tabla 121. Elementos del análisis UDP-Echo	
Elemento	**Descripción**
$authProto	Protocolo de autenticación especificado cuando se creó el elemento.

Tabla 121. Elementos del análisis UDP-Echo (continuación)	
Elemento	**Descripción**
$avgRTT † (AverageRTT)	Tiempo medio de ida y vuelta en segundos.
$community	Comunidad utilizada para enviar solicitudes de SNMP al SAA.
$errBusies	Número de pings que han fallado debido a un ping incompleto anterior.
$ErrDrops	Número de pings que han fallado porque el recurso interno no estaba disponible.
$errTimeouts	Número de pings que han fallado en los tiempos de espera.
$errTotal † (ErrorTotal)	Número total de paquetes con errores.
$errVerifies	Número de pings que ha fallado porque los datos recibidos no eran los mismos que los datos esperados.
$maxRTT † (MaximumRTT)	Tiempo máximo de ida y vuelta en segundos.
$minRTT † (MinimumRTT)	Tiempo mínimo de ida y vuelta en segundos.
$numRTT †	Número de viajes de ida y vuelta correctos.
$port	Puerto utilizado para conectarse con el SAA.
$privProto	Protocolo de privacidad especificado cuando se creó el elemento.
$probeType	udp-echo
$securityName	Nombre de usuario de seguridad especificado cuando se creó el elemento.
$snmpVersion* (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
$sumOfRTT	Suma de todos los tiempos de viaje de ida y vuelta (en segundos).
$targetHost (Host)	Nombre de host del servicio que se supervisa.
$tos (Tos)	Tipo del valor del servicio.
$vpn (Vpn)	Nombre de la VPN.

Nota: † indica que el elemento está disponible para las clasificaciones del nivel de servicio.

Análisis VOIP
Los análisis VOIP generan los mismos elementos que los análisis Jitter. Además, generan los elementos que se listan en la tabla siguiente.

En la tabla siguiente se describen los elementos de análisis de VOID.

Tabla 122. Elementos del análisis VOIP	
Elemento	**Descripción**
$authProto	El protocolo de autenticación especificado cuando se creó el elemento.
$avgRTT † (AverageRTT)	El tiempo medio de ida y vuelta en segundos.
$community	La comunidad utilizada para enviar solicitudes de SNMP al SAA.
$errTotal † (ErrorTotal)	El número total de paquetes con errores.
$ICPIF †	El valor ICPIF.
$maxRTT † (MaximumRTT)	El tiempo máximo de ida y vuelta en segundos.
$minRTT † (MinimumRTT)	El tiempo mínimo de ida y vuelta en segundos.
$MOS †	El valor del Mean Opinion Score (MOS) de la prueba.
$port	El puerto utilizado para conectarse con el SAA.
$privProto	El protocolo de privacidad especificado cuando se creó el elemento.
$probeType †	voip
(ResponderRouter)	El nombre del direccionador que se utiliza para responder a las solicitudes de VOIP.
$securityName	El nombre de usuario de seguridad especificado cuando se creó el elemento.
$snmpVersion (SnmpVersion)	La versión de SNMP utilizada para enviar paquetes SNMP (versión 1, 2c o 3).
(SourceRouter)	El nombre del direccionador que se utiliza para enviar las solicitudes de VOIP.
(Tos)	El tipo del valor del servicio.
(Vpn)	El nombre de la VPN.

Nota: † indica que el elemento está disponible para las clasificaciones del nivel de servicio.

Mensajes de estado
El supervisor SAA proporciona mensajes de estado en el atributo **ResultMessage** cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado de los supervisores SAA.

Tabla 123. Mensajes de estado de supervisor SAA	
Mensaje	**Descripción**
Success (Éxito)	La operación de análisis se ha realizado correctamente.

Tabla 123. Mensajes de estado de supervisor SAA (continuación)	
Mensaje	**Descripción**
`Operation failed` (Operación fallida)	La operación de análisis ha fallado.
`Invalid status` (Estado no válido)	La operación de análisis ha fallado con un estado no válido.

Supervisor SIP

El supervisar SIP comprueba la disponibilidad de los servidores SIP (Session Initiation Protocol - Protocolo de iniciación de sesiones), incluyendo el tiempo necesario para registrar y autenticar los puntos finales. El supervisor inicia una sesión SIP de manera que se puedan supervisar las solicitudes SIP y las respuestas SIP.

En la tabla siguiente se enumeran los archivos de supervisor SIP.

Tabla 124. Resumen de archivos del supervisor SIP	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_sip`
Archivo de propiedades	`$ISHOME/etc/props/sip.props`
Archivo de reglas	`$ISHOME/etc/rules/sip.rules`
Archivo de registro	`$ISHOME/log/sip.log`

Directrices para configurar el supervisor SIP

El supervisor SIP prueba la disponibilidad de un servidor SIP enviando una solicitud al URI de un dispositivo habilitado para SIP, por el servidor SIP, y recibir, también por el servidor SIP, respuestas del dispositivo SIP.

El supervisor SIP actúa como un Cliente de agente de usuario (UAC); inicia las conexiones que se utilizan para probar los servicios SIP. El Servidor de agentes de usuario (UAS), el receptor o el destino de la llamada pueden ser cualquier dispositivo habilitado para SIP como, por ejemplo, un sistema que ejecute un softphone, o un banco de mensajes.

Cuando se prueba un servidor SIP, el supervisor emprende la siguiente secuencia de acciones:

1. Registrarse en el servidor SIP utilizando las credenciales proporcionadas en el elemento de perfil.
2. Enviar una solicitud OPTIONS al UAS.
3. Enviar una solicitud INVITE al UAS.

   Registrar un resultado de la prueba satisfactorio si el UAS acepta la solicitud.
4. Enviar una solicitud BYE al UAS y finalizar la conexión con el UAS.
5. Anular el registro del servidor SIP, con caducidad inmediata.

El supervisor registra la duración de cada acción que se realiza en la prueba.

Propiedades

Las opciones de propiedades específicas para el supervisor SIP se describen en la tabla siguiente.

Tabla 125. Opciones de propiedades del supervisor SIP		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
ShowZeroes	0|1	Especifica la visualización de estadísticas de SIP con valores de cero. 0 - inhabilitado 1 - habilitado
Transports	serie	Lista los transportes de puerto de protocolo local separados por un espacio que es TCP o UDP para el protocolo. Se permiten comodines como números de puerto. Valor predeterminado: UDP:*.

Suites de cifrado

La propiedad **SSLCipherSuite** especifica la suite de cifrado utilizada el supervisor SIP. Para obtener más información, consulte "Establecimiento de SSL en Internet Service Monitoring" en la página 454.

Configuración de pruebas de servicios del supervisor SIP

Utilice los parámetros de configuración del supervisor SIP para definir pruebas de servicios.

Tabla 126. Configuración del supervisor SIP	
Campo	**Descripción**
server	Especifica el nombre del servidor que se va a probar. Por ejemplo, `sip1.mycompany.com`.
serverport	Puerto por el que el supervisor SIP puede alcanzar el servidor que va a ser probado.
username	Especifica el número de extensión o identidad de cuenta del supervisor SIP que realiza la llamada. Por ejemplo, `jblogg`.
target	Especifica el número de extensión de un dispositivo habilitado para SIP que se utiliza para realizar una llamada. Por ejemplo, 5551234.
password	Especifica la contraseña para el nombre de usuario.
description	Campo de texto que proporciona información descriptiva sobre el elemento. Por ejemplo, `Supervisor SIP`.
proxy	Nombre de host del servidor proxy. Por ejemplo, `proxy.mycompany.com`.
proxyport	Puerto por el que el supervisor SIP puede alcanzar el servidor proxy.
timeout	Tiempo de espera, en segundos, para que responda el servidor. Valor predeterminado: 30
poll	Tiempo, en segundos, entre cada sondeo. Valor predeterminado: 300

Tabla 126. Configuración del supervisor SIP (continuación)	
Campo	**Descripción**
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: 0
retestinterval	Tiempo de espera, en segundos, entre cada repetición de prueba tras una anomalía. Valor predeterminado: 10

Clasificación de nivel de servicio

Las clasificaciones del nivel de servicio definen las reglas para determinar el nivel de servicio que se suministra a través de SIP.

Las opciones de clasificación del nivel de servicio disponibles para el supervisor SIP son estas:

```
totalTime
message
```

En las clasificaciones del nivel de servicio:

- Especifique más clasificaciones de nivel de servicio entrando manualmente el nombre del elemento supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección Elementos de supervisor.
- `message` puede ser cualquier mensaje que se reenvíe en el elemento **`$message`** al servidor IBM Application Performance Management si se utiliza en cualquier widget. Para obtener una lista de valores posibles, consulte Mensajes de estado.
- El operando es una serie o un número positivo.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor SIP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio SIP.

En la tabla siguiente se describen los elementos adicionales para el supervisor SIP.

Tabla 127. Elementos del supervisor SIP	
Elemento	**Descripción**
$AcceptReg	Número de solicitudes de registro SIP aceptadas.
$AuthTime* (AuthenticationTime)	Tiempo que se tarda en autorizar tanto el supervisor SIP como el dispositivo habilitado con SIP.
$authAttempts	Número de veces que el supervisor ha necesitado para reenviar una solicitud para incluir sus credenciales.
(CallSetupTime)	Tiempo que se tarda en configurar una llamada.
$Invalid	Número de solicitudes enviadas y recibidas no válidas.

Tabla 127. Elementos del supervisor SIP (continuación)	
Elemento	**Descripción**
$InvalidReg	Número de solicitudes de registro SIP no válidas.
$lastMethod	Último método que ha visto el supervisor, que no sea BYE o ACK.
$lastSequence [MÉTODO]	Última secuencia que se recibe para un método.
$lastStatus [MÉTODO]	Último estado que se recibe para un método o global.
$method *MÉTODO*	Total de mensajes visualizados para un método.
$optionsTime* (OptionsTime)	Tiempo que se tarda en negociar un cambio de opciones (de OPTIONS a 200 OK).
$postDialTime* (PostDialTime)	Tiempo que se tarda en recibir una señal sonora después del marcado (INVITE a 180 Llamando).
$RegTime* (RegistrationTime)	Tiempo que se tarda en registrar tanto el supervisor SIP como el dispositivo habilitado con SIP.
$registrationTime	Tiempo que se tarda en registrarse con el servidor (de REGISTER a 200 OK).
$Requests	Número de mensajes de solicitud de SIP recibidos y enviados.
($RequestsSent)	Número de mensajes de solicitudes SIP enviados.
`${request|response}[Sent|Received|Transmitted|Total][METHOD][STATUS]`	Total de mensajes vistos para varias categorías, por ejemplo, `requestSentINVITE = 1`, `responseReceived = 10` y `responseReceivedBYE200 = 1`.
$Responses	Número de mensajes de respuesta de SIP recibidos y enviados.
($ResponseReceived)	Número de mensajes de respuesta SIP recibidos.
$sessionAnswered	• 1 - si se responde a la llamada • 0 - si no se responde a la llamada
$sessionCreated	• 1 - si se establece una sesión • 0 - si no se establece una sesión

Tabla 127. Elementos del supervisor SIP (continuación)	
Elemento	**Descripción**
$sessionTerminated	• 1 - si la sesión finaliza • 0 - si la sesión no finaliza.
$shutdownTime* (ShutdownTime)	El tiempo que se tarda en finalizar la conexión (de BYE a 200 OK).
$terminatedReason* (TerminatedReason)	Razón del cierre de la conexión.
(Username)	Nombre de usuario utilizado para iniciar la sesión en el servidor SIP.
(Target)	Destino en el que abrir la sesión.

Mensajes de estado

El supervisor SIP proporciona mensajes de estado en el atributo **ResultMessage** cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado del supervisor SIP.

Tabla 128. Mensajes de estado de supervisor SIP	
Mensaje	**Descripción**
`Register timed out` (se ha excedido el tiempo de espera de registro)	El supervisor no ha podido registrarse en el servidor.
`Invite timed out` (Se ha superado el tiempo de espera de INVITE)	Se ha superado el tiempo de espera del mensaje INVITE.
OK (CORRECTO)	La solicitud y la respuesta han sido correctas.
`n operation status description` (descripción del estado de la operación n)	• *n* es la secuencia de numeración del mensaje. • operation es el tipo de mensaje. • status es el código de estado. • description es una descripción del estado en texto sin formato. Por ejemplo, `1 INVITE 200 OK`.

Respuestas de SIP

El supervisor SIP admite los siguientes tipos de respuestas. Cada respuesta tiene un código de 3 dígitos:

- Respuestas informativas (100-199)
- Respuestas satisfactorias (200 - 299)
- Respuestas de redirección (300-399)
- Respuestas de anomalía de cliente (400-499)
- Respuestas de anomalía de servidor (500-599)

- Respuestas de anomalía global (600-699)

En la tabla siguiente se listan las respuestas SIP habituales.

Tabla 129. Respuestas de SIP habituales	
Respuesta	**Descripción**
100 Trying (Intentando)	El dispositivo habilitado para SIP recibe el mensaje pero éste aún se debe procesar.
180 Ringing (Llamando)	El dispositivo habilitado para SIP recibe y procesa el mensaje. El dispositivo está llamando para alertar al usuario.
200 OK (Correcto)	Este código se devuelve cuando se completa correctamente un método. Por ejemplo, la llamada se ha registrado en el servidor o el usuario ha respondido la llamada.
401 Unauthorized (No autorizado)	El usuario no tiene autorización.
407 Proxy Authentication Required (Se requiere autenticación de proxy)	Este código es parecido al 401, pero indica que el usuario debe autenticarse primero.
408 Request Timeout (Tiempo de espera de petición excedido)	El usuario no ha respondido a la llamada.

Para obtener una lista completa de respuestas SIP, consulte RFC3261.

Supervisor SMTP

El supervisor SMTP trabaja junto con los supervisores IMAP4 o POP3 para probar el rendimiento de un servicio de correo electrónico.

En la tabla siguiente se listan los archivos de supervisor SMTP.

Tabla 130. Archivos del supervisor SMTP	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_smtp`
Archivo de propiedades	`$ISHOME/etc/props/smtp.props`
Archivo de reglas	`$ISHOME/etc/rules/smtp.rules`
Archivo de registro	`$ISHOME/log/smtp.log`

Directrices para configurar el supervisor SMTP

El supervisor SMTP funciona junto con los supervisores POP3 o IMAP4. Periódicamente envía un mensaje de correo electrónico a un buzón en el servidor de destino y registra el tiempo que se tarda en emitir la solicitud de correo electrónico. A continuación, el supervisor POP3 o IMAP4 lee los mensajes del buzón y los utiliza para calcular el tiempo de respuesta y la disponibilidad del servicio de correo electrónico.

Nota: El supervisor SMTP funciona junto con los supervisores POP3 o IMAP4. Periódicamente envía un mensaje de correo electrónico a un buzón en el servidor de destino y registra el tiempo que se tarda en emitir la solicitud de correo electrónico. A continuación, el supervisor POP3 o IMAP4 lee los mensajes del buzón y los utiliza para calcular el tiempo de respuesta y la disponibilidad del servicio de correo electrónico.

Buzones

Puede configurar el supervisor para que envíe mensajes de correo electrónico a cualquier buzón existente, incluso si el buzón pertenece a un usuario real. Sin embargo, es aconsejable crear una cuenta de buzón especial para la prueba de servicio. El parámetro de correo electrónico especifica el buzón del destinatario. De forma predeterminada, el supervisor envía mensajes de prueba con la línea de asunto `Mensaje de prueba de supervisor SMTP`. Si es necesario, puede configurar los elementos de perfil SMTP sin un nombre de buzón. En esta configuración, el supervisor simplemente comprueba que el servicio SMTP acepte conexiones.

Correos seguros

El supervisor SMTP admite conexiones a servicios de correo seguro. Se puede conectar utilizando SSL/TLS, o el mandato STARTTLS. Cuando defina un elemento del supervisor SMTP, utilice el campo Tipo de seguridad para seleccionar la seguridad adecuada. Si el servidor de correo requiere un certificado del lado del cliente para el cifrado SSL, utilice las propiedades o las opciones de la línea de mandatos de SSLname para especificar un archivo de certificado, un archivo de claves, una contraseña de clave y una suite de cifrado.

Certificado del lado del cliente

El supervisor SMTP le permite supervisar servidores que requieren certificados del lado del cliente para la autenticación mutua. Al crear un elemento de perfil, debe especificar el archivo de certificados SSL, el archivo de claves y la contraseña de clave. Los certificados deben estar en el formato PEM (Privacy Enhanced Mail). Si el certificado tiene otro formato, debe convertirlo al formato PEM. Puede convertir certificados utilizando software como, por ejemplo, openSSL, que está disponible en http://www.openssl.org.

Nota: Si utiliza siempre el mismo certificado, la misma clave y la misma contraseña en todos los elementos de perfil, especifíquelos utilizando propiedades de supervisor en lugar de definiéndolos en cada elemento de perfil que cree.

Configuración de las pruebas de servicios del supervisor SMTP

Utilice los parámetros de configuración del supervisor SMTP para definir pruebas de servicios. Cuando configura el supervisor, se muestran los valores predeterminados para los parámetros de tiempo de espera excedido e intervalo de sondeo, Estos valores predeterminados son 30 y 300 segundos, respectivamente. Si no se especifica ningún valor los demás valores predeterminados listados en la tabla no se muestran durante la configuración pero se aplican cuando se guardan los detalles de configuración.

Tabla 131. Configuración del supervisor SMTP

Campo	Descripción
server	La dirección IP del servidor de correo. El ejemplo es `mail.mycompany.com`
description	Campo de texto para proporcionar información descriptiva sobre el elemento.
port	Número de puerto del servidor de correo. Valor predeterminado: 25 Si utiliza un servidor que no es un servidor SMTP, actualice el puerto en el que se va a conectar al servidor. Por ejemplo, si utiliza un servidor IMAP4 a través de SSL para Microsoft Exchange, especifique el puerto 465.

Tabla 131. Configuración del supervisor SMTP (continuación)	
Campo	**Descripción**
securitytype	Tipo de conexión segura que se abre con el servidor de correo: • NONE: conectarse sin seguridad. • SSL: enviar hello de SSLv2 y luego negociar SSLv2, SSLv3 o TLSv1. • STARTTLS: conectarse sin seguridad, enviar un mandato STARTTLS y luego establecer una conexión por TLSv1. Valor predeterminado: NONE
username	Nombre de usuario que se utiliza para iniciar la sesión en el servidor SMTP. Se utiliza con autenticación PLAIN o CRAM-MD5.
password	Contraseña que se utiliza para iniciar la sesión en el servidor SMTP. Se utiliza con autenticación PLAIN o CRAM-MD5.
authenticationtype	Método para autenticar el supervisor en el servidor SMTP. Las opciones disponibles son: • NONE: no se intenta ninguna autenticación • PLAIN: autenticación de nombre de usuario y contraseña con texto sin formato • CRAM-MD5: se utiliza la autenticación CRAM-MD5 El valor predeterminado es NONE.
sharedsecret	Clave secreta compartida para la autenticación CRAM-MD5.
email	La dirección de correo electrónico del buzón utilizado por los supervisores SMTP y POP3.
timeout	Tiempo, en segundos, que se debe esperar a que el servidor SMTP responda. Valor predeterminado: 30
poll	El tiempo, en segundos, entre cada sondeo. Valor predeterminado: 300
failureretests	El número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: 0
retestinterval	El tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: 10

Nota: Supervise la disponibilidad del servidor de correo mail.mycompany.com intentando conectarse a él a intervalos de diez minutos. Utilice un tiempo de espera de conexión de 30 segundos y, si la conexión da error, vuélvalo a intentar tres veces con un intervalo de cinco segundos entre cada reintento.

Elemento del supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor SMTP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio SMTP.

En la tabla siguiente se describen los elementos adicionales para el supervisor SMTP.

Tabla 132. Elementos del supervisor SMTP

Elemento	Descripción
$authentication	El tipo del método de autenticación de usuario necesario para el servidor SMTP (Standard o APOP).
$bytesPerSec	Número promedio de bytes transferidos cada segundo.
$bytesTransferred	El número de bytes cargados o descargados.
$connectTime* (ConnectTime)	Tiempo que se tarda en conectar con el servidor SMTP.
$email* (EmailAddress)	La dirección de correo electrónico del buzón al que el supervisor envía correo electrónico de prueba.
$lookupTime* (LookupTime)	El tiempo que se tarda en obtener la dirección IP del servidor de host.
$port* (Port)	Puerto en que se supervisa el servicio.
$responseTime* (ResponseTime)	El tiempo que se tarda, después de crear una conexión, hasta que el primer byte del correo electrónico de prueba puede enviarse al servidor SMTP.
$security	El tipo de conexión segura abierta con el servidor de correo (NONE, STARTTLS o SSL) como se establece en el campo **securitytype** del elemento de perfil.
$SSLHandshakeTime* (SslHandshakeTime)	El tiempo que se tarda en establecer la conexión SSL.
$status* (ResultStatus)	El código de estado devuelto por el servidor SMTP.
$uploadTime* (UploadTime)	El tiempo que se tarda en cargar el archivo.
$user* (SmtpUser)	El nombre de usuario (nombre de cuenta) utilizado por el supervisor para iniciar la sesión en el servidor SMTP.

Mensaje de estado

El supervisor SMTP proporciona mensajes de estado en el elemento $message cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

Propiedades

Las propiedades específicas del supervisor SMTP se describen en la tabla siguiente.

Tabla 133. Propiedades y opciones de la línea de mandatos del supervisor SMTP

Nombre de propiedad	Parámetro de propiedad	Descripción
`MailMessage Path`	serie	Vía de acceso a un archivo que contiene texto para enviar en el correo electrónico de prueba. Si no se ha establecido, se envía un mensaje predeterminado.
`Originator`	serie	Especifica el campo De que se debe establecer al enviar el correo electrónico de prueba. Asegúrese de que coincida con la cadena correspondiente del supervisor IMAP4. Valor predeterminado: `SMTP-Monitor`.
`SSLCertificate File`	serie	La vía de acceso y el nombre de archivo del archivo de certificado digital utilizado si no se especifica ningún certificado de forma explícita para un elemento SMTP durante su creación. Si la vía de acceso no es absoluta, el supervisor lo interpreta como relativo al directorio de trabajo, (`$ISHOME/platform/arch/bin`).
`SSLCipherSuite`	serie	La suite de cifrado que se utiliza para las operaciones SSL. Para obtener una descripción de los valores posibles, consulte Suites de cifrado. Valor predeterminado: `RC4:3DES:DES:+EXP`
`SSLDisableTLS`	entero	Inhabilita TLSv1 para el soporte de legado. Valor predeterminado: `0` - TLSv1 está habilitado. 1 TLSv1 está inhabilitado.
`SSLKeyFile`	serie	El archivo que contiene la clave privada SSL.
`SSLKeyPassword`	serie	La contraseña utilizada para cifrar la clave privada SSL.
`UseBody`	entero	Especifica donde el supervisor escribe información de seguimiento en el mensaje de correo, ya sea en la cabecera del correo o en el cuerpo del correo. Valor predeterminado: `0` - se incluye información en la cabecera de correo. 1 - escribir información en el cuerpo de mensaje de correo.

Suites de cifrado

La propiedad `SSLCipherSuite` especifica el conjunto de cifrado utilizado por el supervisor SMTP. Para más información sobre valores SSL, consulte "Establecimiento de SSL en Internet Service Monitoring" en la página 454.

Supervisor SNMP

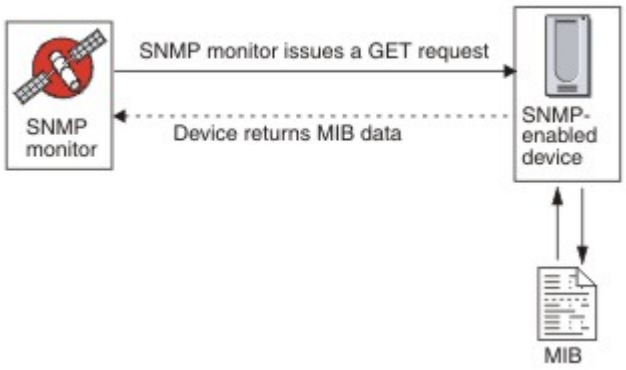
El supervisor SNMP prueba los datos de error y rendimiento de los dispositivos habilitados para SNMP.

En la tabla siguiente se enumeran los archivos de supervisor SNMP.

Tabla 134. Resumen del supervisor SNMP	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_snmp`
Archivo de propiedades	`$ISHOME/etc/props/snmp.props`
Archivo de reglas	`$ISHOME/etc/rules/snmp.rules`
Archivo de registro	`$ISHOME/log/snmp.log`

Directrices para configurar el supervisor SNMP

El supervisor SNMP adquiere datos de dispositivos habilitados para SNMP enviando solicitudes GET de SNMP para uno o más objetos contenidos en el MIB de un dispositivo. A continuación, el dispositivo devuelve los datos MIB al supervisor SNMP. El supervisor SNMP da soporte a las versiones 1, 2c y 3 de SNMP.



Propiedades

Las opciones de propiedades específicas para el supervisor SNMP se describen en la tabla siguiente.

Tabla 135. Opciones de propiedades del supervisor SNMP		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
InvalidBps Value	entero	Especifica un valor entero sustituido para los cálculos de valores de bits por segundo (Bps) cuando sólo hay disponible un punto de datos.
MibDir	serie	Especifica el directorio que contiene los documentos MIB utilizados por el supervisor. Valor predeterminado: `$ISHOME/mibs`.
StripQuotes	`0|1`	Elimina los caracteres de comillas de los datos de enteros. `0` - inhabilitado `1` - habilitado

Tabla 135. Opciones de propiedades del supervisor SNMP (continuación)		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
Umbral de retrotracción	entero	El valor que un delta debe cumplir o superar si se produce una retrotracción antes de que se produzca un restablecimiento del direccionador. Valor predeterminado: 0 (no retrotraer nunca)

Configuración de pruebas de servicios del supervisor SNMP

Utilice los parámetros de configuración del supervisor SNMP para definir pruebas de servicios.

Tabla 136. Configuración del supervisor SNMP	
Campo	**Descripción**
server	Servidor al que enviar solicitudes GET de SNMP.
objectgroupname	Nombre de texto para el grupo de OID que se desea incluir en la solicitud GET.
communitystring	Serie de comunidad de lectura/escritura de SNMP para el servidor SNMP en el cliente. **Nota:** Utilice con cuidado el carácter de acento circunflejo (^) en los nombres de comunidad; consulte Nombres de comunidad para obtener más información.
description	Campo de texto para proporcionar información descriptiva sobre el elemento.
port	Puerto del servidor que se va a utilizar. Valor predeterminado: 161
version	Versión de SNMP que se va a utilizar: 1 - SNMPv1 2 - SNMPv2c 3 - SNMPv3 Valor predeterminado: 1
securityname†	Nombre de usuario para la sesión SNMP.
authenticationphrase†	Contraseña de autenticación para el usuario.
privacyphrase†	Contraseña de privacidad para el usuario.
authenticationprotocol†	Protocolo que se debe utilizar para autenticar el usuario: • MD5 • SHA1 Valor predeterminado: MD5
privacyprotocol†	Protocolo que se debe utilizar para cifrar la sesión. Valor predeterminado: DES

Tabla 136. Configuración del supervisor SNMP (continuación)

Campo	Descripción
timeout	Tiempo de espera, en segundos, para que responda el servidor. Valor predeterminado: 20
poll	Tiempo, en segundos, entre cada sondeo. Valor predeterminado: 300
retries	Número de veces que el supervisor reintenta contactar con el direccionador antes de efectuar la salida. Valor predeterminado: 0
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: 0
retestinterval	Tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: 10
hostnamelookuppreference	Determina qué versión de IP, IPv6 o IPv4, se aplica al nombre de host proporcionado. Las opciones son: • `default` define el supervisor para utilizar valores de propiedades de nivel de supervisor. Es el valor predeterminado. • `4Then6` selecciona IPv4 y, después, IPv6. Utiliza direcciones IPv4 si están disponibles. Si no se encuentra ninguna dirección IPv4, se utilizan direcciones IPv6. • `6Then4` seleccione IPv6 y, después, IPv4. Utiliza direcciones IPv6 si están disponibles. Si no se ha encontrado ninguna dirección IPv6, se utilizan direcciones IPv4. • `4Only` solo selecciona IPv4. Solo utiliza direcciones IPv4. Si no hay ninguna dirección IPv4, el sondeo devuelve un error. • `6Only` solo selecciona IPv6. Solo utiliza direcciones IPv6. Si no hay ninguna dirección IPv6, el sondeo devuelve un error. • `6or4` selecciona IPv4 o bien IPv6. Utiliza la primera dirección devuelta desde el nombre de host.
† Sólo aplicable a SNMPv3.	

Nombres de comunidad

Internet Service Monitoring utiliza el carácter de acento circunflejo (^) como carácter de escape al enviar información al dispositivo de destino. Si un nombre de comunidad contiene un acento circunflejo, debe especificar dos acentos circunflejos en una fila (^^) para que el nombre sea correcto en el direccionador. Por ejemplo, para que el nombre de comunidad a$^&b sea correcto cuando se envía al dispositivo, utilice a$^^&b.

Clasificaciones de nivel de servicio

Las clasificaciones del nivel de servicio definen las reglas para determinar el nivel de servicio.

Las opciones de clasificación del nivel de servicio disponibles para el supervisor SNMP son estas:

```
totalTime
message
```

En las clasificaciones del nivel de servicio.

- Especifique más clasificaciones de nivel de servicio entrando manualmente el nombre del elemento supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección Elementos de supervisor.
- `message` puede ser cualquier mensaje que se reenvíe en el elemento **$message** al servidor IBM Application Performance Management si se utiliza en cualquier widget. Para obtener una lista de valores posibles, consulte Mensajes de estado.
- El operando es una serie o un número positivo.
- oidName es el nombre que se asigna a un objeto de MIB en el campo Nombre de OID definido en el grupo de OID.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor SNMP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio SNMP.

En la tabla siguiente se describen los elementos adicionales para el supervisor SNMP.

Tabla 137. Elementos del supervisor SNMP

Elemento	**Descripción**
$community	Serie de comunidad de SNMP para el servidor SNMP en el cliente.
$numOids	Número de OIDs utilizados en la consulta.
$oidGroupName* (OidGroup)	Nombre del grupo de OID. El grupo de OID contiene los OID que está sondeando el supervisor.
$oidName*0 a n** (OIDName*Cero a nueve*)	Nombre del primer al último objeto MIB del grupo de OID. Se indica mediante un número al utilizar Netcool/OMNIbus y con texto alfabético (de cero a nueve) al utilizar IBM Application Performance Management.
$oidNames	Nombres de cada OID separados por una barra vertical (|).
$oidReturnValues*0 a n** (snmpResult*Cero a nueve*)	Los datos que devuelve el mandato GET de SNMP para el primer al último objeto MIB del grupo de OID. Se indica mediante un número al utilizar Netcool/OMNIbus y con texto alfabético (de cero a nueve) al utilizar IBM Application Performance Management.
$oidUnit*0 a n*	Unidades para del primer al último objeto MIB del grupo de OID indicado por un número.
$oidUnits	Unidades para cada OID, separados por un carácter de barra vertical (|).
$port	Puerto en que se supervisa el servicio.
$snmpVersion* (SnmpVersion)	Versión de SNMP utilizada para enviar paquetes de SNMP configurados en el perfil (Versión 1, 2c o 3).

Mensajes de estado

El supervisor SNMP proporciona mensajes de estado en el atributo `ResultMessage` cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado del supervisor SNMP.

Tabla 138. Mensajes de estado de supervisor SNMP

Mensaje	**Descripción**
`Successful Get` (Get correcto)	La consulta del agente SNMP ha sido satisfactoria.
`Failed to open snmp sessions` (No se han podido abrir las sesiones SNMP) `SNMP session - start failed` (El inicio de sesión de SNMP ha fallado)	No se puede inicializar una sesión SNMP.
`Error in packet` (Error en paquete)	No se ha podido crear un paquete SNMP válido.
`Timed out while waiting for response` (Se ha excedido el tiempo de espera al esperar una respuesta)	No se ha recibido ninguna respuesta del agente SNMP.
`Internal Error` (Error interno)	Se ha producido un error interno en el supervisor. Para obtener más información, póngase en contacto con el soporte técnico de IBM.
`Error Processing OID` (Error de proceso de OID)	Se ha producido un error al procesar uno de los `OID`.
`ERROR: Too Many OIDs` (ERROR: hay demasiados OID)	El supervisor se ha establecido para solicitar demasiados `OID` a la vez. El máximo es `100`.
`ERROR: PDU received mismatch with PDU sent` (ERROR: la PDU recibida discrepa con una PDU enviada)	La unidad de datos de protocolo (PDU) recibida por el supervisor no coincidía con la PDU enviada al servidor.

Supervisor SOAP

El supervisor SOAP comprueba la disponibilidad y el tiempo de respuesta de la interfaz SOAP (SOAP 1.0 y 1.1). También puede supervisar la validez de las entradas de SOAP (solicitudes) y las salidas de SOAP (respuestas).

El supervisor SOAP admite los estilos de codificación de mensajes siguientes:

- RPC: codificado
- Documento: literal sin ajustar
- Documento: literal ajustado

En la tabla siguiente se enumeran los archivos de supervisor SOAP.

Tabla 139. Resumen de archivos de supervisor SOAP

Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_soap`

Tabla 139. Resumen de archivos de supervisor SOAP (continuación)	
Archivos de supervisor	**Nombre o ubicación**
Archivo de propiedades	`$ISHOME/etc/props/soap.props`
Archivo de reglas	`$ISHOME/etc/rules/soap.rules`
Archivo de registro	`$ISHOME/log/soap.log`

Directrices para configurar el supervisor SOAP

El supervisor SOAP prueba la operación de un servicio SOAP enviando a la interfaz SOAP de destino una solicitud que contiene un conjunto de entradas y, a continuación, recibiendo y analizando las salidas que están contenidas en la respuesta que se recibe de la interfaz. Cuando se envía una solicitud a la interfaz SOAP, la solicitud puede realizarse correctamente o fallar. Una solicitud es satisfactoria si se recibe una respuesta y los valores del mensaje de respuesta coinciden con los valores de salida especificados. Una solicitud falla si no se recibe ninguna respuesta o si se recibe una respuesta pero los valores de su mensaje no coinciden con los valores de salida.

Las entradas y salidas de SOAP que están contenidas en las solicitudes y respuestas dependen de las funciones del servicio SOAP a prueba; cuando diseñe una prueba para un servicio SOAP, debe especificar entradas y salidas apropiadas para dicho servicio. Las entradas consisten en los nombres de los datos que se van a enviar y sus valores de entrada asignados. Las salidas consisten en los nombres de los datos que se van a recibir y sus valores de salida esperados. Estos nombres de datos se originan en un archivo de Lenguaje de descripción de servicios web (WSDL) local, que se especifica al configurar el supervisor SOAP. Los nombres de datos de entrada y salida deben coincidir con los de los tipos de datos del archivo WSDL. Los nombres de datos deben estar también en el mismo orden que en el archivo WSDL. Si los nombres no coinciden, o si el orden es incorrecto, se genera un mensaje de error cuando el supervisor intenta sondear la interfaz SOAP.

El formato de las entradas es:

```
nombre_datos:tipo_datos=valor_asignado,nombre_datos:tipo_datos=valor_asignado, ...
```

El formato de las salidas es:

```
nombre_datos:tipo_datos=valor_esperado,
nombre_datos:tipo_datos=valor_esperado, ...
```

Tipos de datos SOAP

El supervisor SOAP admite tipos de datos simples, de matriz y definidos por los usuarios. Los tipos de datos simples incluyen Entero, Serie y Booleano. Las matrices pueden contener tipos de datos simples y otros tipos de datos de matriz y definidos por el usuario.

Tabla 140. Tipos de datos simples			
Tipos de datos simples			
anyURI	float	language	Qname
booleano	gDay	long	short
byte	gMonth	Nombre	string
date	gMonthDay	NCName	time
dateTime	gYear	negativeInteger	token

Tabla 140. Tipos de datos simples (continuación)			
Tipos de datos simples			
decimal	gYearMonth	NMTOKEN	unsignedByte
double	ID	NMTOKENS	unsignedInt
duration	IDREFS	nonNegativeInteger	unsignedLong
ENTITIES	int	nonPostiveInteger	unsignedShort
ENTITY	integer	normalizedString	

Autenticación SOAP

Si la interfaz SOAP que desea supervisar necesita la autenticación HTTP básica, especifique las credenciales para acceder a la interfaz en el elemento de perfil SOAP cuando utilice la herramienta de configuración de Internet Service Monitoring.

Para establecer los parámetros de autenticación SOAP necesarios:

1. En la herramienta de configuración de Internet Service Monitoring, seleccione el elemento de perfil para el que desee añadir información de autenticación.
2. En la pestaña **Avanzado**, pulse el campo **Valor** para el parámetro `username` y especifique el valor necesario.
3. Pulse el campo **Valor** para el parámetro `password` y especifique el valor necesario. La contraseña está cifrada.
4. Pulse **Aceptar**.

Si la autenticación ya no es necesaria, suprima los valores de los parámetros **`username`** y **`password`**.

Propiedades

Las opciones de propiedades específicas para el supervisor SOAP se describen en la tabla siguiente.

Tabla 141. Opciones de propiedades del supervisor SOAP			
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**	**Valor predeterminado**
SoapParser	serie	Biblioteca de análisis de XML.	`$ISHOME/platform/$ARCH/bin/AxisXMLParserXerces.dll`
SoapTransport	serie	Biblioteca de transporte de SOAP.	`$ISHOME/platform/$ARCH/bin/HTTPTransport.dll`
SoapChannel	serie	Biblioteca de canales SOAP.	`$ISHOME/platform/$ARCH/bin/HTTPChannel.dll`
SoapSecureChannel	serie	Biblioteca de canales seguros SOAP.	`$ISHOME/platform/$ARCH/bin/HTTPSSLChannel.dll`
SoapClientLog	serie	El nombre del archivo de registro de cliente SOAP adicional.	`$ISHOME/log/SoapClient.log`

Suites de cifrado

La propiedad SSLCipherSuite especifica la suite de cifrado utilizada por el supervisor SOAP.

Para obtener más información, consulte “Establecimiento de SSL en Internet Service Monitoring” en la página 454.

Configuración de pruebas de servicios del supervisor SOAP

Utilice los parámetros de configuración del supervisor SOAP para definir pruebas de servicios.

Tabla 142. Configuración del supervisor SOAP

Elemento	**Descripción**
wsdl	Vía de acceso de la copia local del archivo WSDL.
operation	Nombre de la operación SOAP.
operationnamespace	Espacio de nombre de la operación SOAP.
location	URL del servicio SOAP que se va a supervisar.
description	Campo de texto para proporcionar información descriptiva sobre el elemento.
timeout	Tiempo, en segundos, que se debe esperar a que el servicio SOAP responda. Valor predeterminado: 10
poll	Tiempo, en segundos, entre cada sondeo. Valor predeterminado: 300
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: 0
retestinterval	Tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: 10
Parámetros de SOAP	
inputs	Proporciona acceso a los campos de nombre, tipo y valor, incluidos los atributos, para entradas de SOAP. Puede utilizar parámetros de soap simples, complejos o matriciales. Por ejemplo: • Simple: symbol:string="IBM" • Complejo: outer:{item1:string,item2:string}**(aaa:string='bbb')** ={item1**(attr:string='ccc')**='', item2**(attr:string='ddd',attr2:string='eee')**='fff'} En este ejemplo, los atributos entre paréntesis, marcados en negrita, son opcionales. • Matriz: input:int[]=[1,2,3,4]

Tabla 142. Configuración del supervisor SOAP (continuación)	
Elemento	**Descripción**
outputs	Proporciona acceso a los campos de nombre, tipo y valor, incluidos los atributos, para salidas de SOAP. Utilice parámetros de SOAP simples, complejos o de matriz. Para obtener más información sobre la sintaxis, consulte los ejemplos de las entradas de parámetros SOAP.

Clasificación de nivel de servicio

Las clasificaciones del nivel de servicio definen las reglas para determinar el nivel de servicio suministrado por la interfaz SOAP.

Las opciones de clasificación del nivel de servicio disponibles son estas:

```
totalTime
message
```

En las clasificaciones del nivel de servicio:

- Especifique más clasificaciones de nivel de servicio entrando manualmente el nombre del elemento supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección Elementos de supervisor.
- `message` puede ser cualquier mensaje en el elemento **`$message`** al servidor de IBM Application Performance Management si se utiliza en cualquier widget. Para obtener una lista de valores posibles, consulte Mensajes de estado.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor SOAP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio SOAP.

En la tabla siguiente se indican los elementos adicionales para el supervisor SOAP.

Tabla 143. Elementos de supervisor de SOAP	
Elemento	**Descripción**
(Location)	URL del servicio SOAP que se supervisa.
(Operation)	Nombre del servicio SOAP que se supervisa.
$outputMatch	`Success` si el valor devuelto coincide con el valor de salida; de lo contrario, `Failure`.
$responseValueName	Nombre de valor recibido en la respuesta de SOAP.
$soapname	Nombre de contenedor de la respuesta de SOAP. Sólo aplicable a tipos de datos complejos definidos por el usuario y de matriz.
$soaptype	Tipo de contenedor de la respuesta de SOAP. Sólo aplicable a tipos de datos complejos definidos por el usuario y de matriz.
(WSDL)	Vía de acceso de la copia local del archivo WSDL.

Mensajes de estado

El supervisor SOAP proporciona mensajes de estado en el atributo **`ResultMessage`** cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

Los mensajes son Success si los valores devueltos coinciden con los valores de salida o un mensaje de error. El mensaje de error contiene una descripción del error.

Ejemplo

Supervise la disponibilidad de la interfaz SOAP a intervalos de 5 minutos. Si la interfaz SOAP no está disponible, repita la prueba como máximo dos veces, dejando 5 segundos entre cada prueba repetida. Envíe una solicitud que añada 1 + 2 y compruebe que la respuesta contiene el valor de 3.

Cree un elemento de perfil SOAP y establezca los campos que se muestran en la tabla siguiente.

Tabla 144. Ejemplo de elemento de perfil SOAP

Campo de configuración	**Valor**
wsdl	`c:\%ISMHOME%\etc\SOAP.wsdl`
operation	add
operationnamespace	`http://localhost/SOAP/Calculator`
location	`http://serverA/SOAP/Calculator`
description	basic Calculator SOAP monitor
Active	Seleccionado
timeout	30
poll	300
failureretests	2
retestinterval	5
inputs	[in0=1,in1=2]
outputs	[addReturn=3]

Supervisor TCPPort

El supervisor TCPPort proporciona cobertura para servicios no probados por los demás supervisores. Detecta y responde a los mandatos o a las cadenas en un puerto TCP. Este supervisor es especialmente útil para supervisar los servicios personalizados.

En la tabla siguiente se enumeran los archivos de supervisión TCPPort.

Tabla 145. Archivos de supervisión TCPPort

Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_tcpport`
Archivo de propiedades	`$ISHOME/etc/props/tcpport.props`
Archivo de reglas	`$ISHOME/etc/rules/tcpport.rules`
Archivo de registro	`$ISHOME/log/tcpport.log`

Directrices para configurar el supervisor TCPPort

El supervisor TCPPort prueba servicios basados en TCP conectándose al servicio, supervisando mensajes recibidos del servicio y enviándole respuestas.

Para configurar una prueba, defina una secuencia de mensajes y respuestas previstas que engloban una interacción normal en ese servicio.

Por ejemplo, una interacción estándar para un servicio telnet implica la secuencia siguiente.

- El servicio telnet envía un mensaje de inicio de sesión, que le solicita un nombre de usuario.
- El cliente envía una respuesta que contiene un nombre de usuario.
- El servicio telnet envía un mensaje que le solicita una contraseña.
- El cliente envía una respuesta que contiene una contraseña.
- Si el intento de inicio de sesión es correcto, el servicio telnet envía algún tipo de mensaje de bienvenida.

Las propiedades **WaitFornn** y **Sendn** del supervisor especificadas definen los mensajes y las respuestas a estos mensajes previstos. Estas propiedades del archivo de propiedades del supervisor, definen cómo interactúa el supervisor con el servicio TCP.

- Las propiedades **WaitFornn** son expresiones regulares. El supervisor las utiliza para comparar los mensajes recibidos en el puerto supervisado.
- Las propiedades **Sendn** son series literales que escribe el supervisor en el puerto.

Nota: Si es necesario, puede insertar caracteres de control en estas propiedades utilizando un editor de texto que admita la inserción de caracteres de control.

El formato para definir las propiedades WaitFornn y Sendn es:

```
WaitFor1: primer mensaje recibido
Send1: primera respuesta
WaitFor2: segundo mensaje recibido
Send2: segunda respuesta
...
WaitFor5: quinto mensaje recibido
Send5: quinta respuesta
```

Cuando el supervisor alcanza la primera propiedad **WaitFor** no establecida, deja de enviar y recibir. Si la propiedad **MonitorDisconnect** está establecida en 0, el servicio supervisado debe cerrar la conexión abierta por el supervisor; de lo contrario, el supervisor notificará el mensaje `Tiempo de espera agotado en la espera para leer` en su elemento **$message**. Con muchos servicios, la conexión se puede cerrar enviando de un mandato `quit`. Si **MonitorDisconnect** está establecido en 1, el supervisor se desconecta después de que se complete el mandato Send o `WaitFor`, o se supere el tiempo de espera, lo que suceda primero.

Configuración de la prueba de servicios de supervisor TCPPort

Utilice los parámetros de configuración de supervisor TCPPort para definir pruebas de servicio.

Tabla 146. Configuración de TCPPort

Campo	Descripción
server	Dirección IP del sistema en el que se está ejecutando el servicio de destino. Por ejemplo, `server.mycompany.com`
port	Puerto en el que se va a conectar al servicio de destino.
description	Campo de texto para proporcionar información descriptiva sobre el elemento.
timeout	Tiempo de espera, en segundos, para que responda el servidor. Valor predeterminado: `30`

Tabla 146. Configuración de TCPPort (continuación)	
Campo	**Descripción**
poll	Tiempo, en segundos, entre cada sondeo. Valor predeterminado: `300`
failureretests	Número de veces que se repetirán las pruebas antes de indicar una anomalía. Valor predeterminado: `0`
retestinterval	Tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: `10`

Nota: Supervise la disponibilidad del servicio `telnet` que se ejecuta en el host `server.mycompany.com` en el puerto 23. Utilice las credenciales `user` o `guest` para iniciar la sesión en el servidor y cierre la conexión inmediatamente después del inicio de sesión. Ejecute la prueba a intervalos de 5 minutos, y establezca un tiempo de espera de 10 segundos en los intentos de conexión.

1.Añada las entradas siguientes al archivo de propiedades TCPPort:

```
WaitFor1: ".*[Ll]ogin:"
Send1: "user"
WaitFor2: ".*[Pp]assword:"
Send2: "guest"
WaitFor3: ".*%"
Send3: "exit"
```

2.Inicie o reinicie el supervisor TCPPort.

Coincidencias de expresiones regulares

Realice una búsqueda de expresiones regulares en la información descargada especificando hasta 50 expresiones regulares diferentes. El supervisor TCPPort intenta hacer coincidir el contenido recuperado con cada una de las expresiones regulares. Si se encuentra una coincidencia para cada una expresión regular especificada, las líneas coincidentes (o todas las que quepan en el almacenamiento intermedio del supervisor) se devuelven en el elemento `$regexpMatchn` correspondiente. Si la expresión regular coincide más de una vez en la información descargada, sólo se devuelve la primera coincidencia. El estado de cada prueba de expresión regular se indica con los elementos `$regexpStatusn`. Puede utilizar las coincidencias de expresiones regulares y su información de estado como criterios para las clasificaciones del nivel de servicios.

Para obtener más información, consulte Tabla 50 en la página 338.

Elementos de supervisor

En la tabla siguiente se describen los elementos adicionales para el supervisor TCPPort.

Los elementos indicados con un asterisco (*) están disponibles como atributos. Los nombres de los atributos se muestran entre corchetes. La ausencia de un asterisco indica que no hay ningún atributo equivalente. Los atributos que se muestran entre corchetes, pero sin un elemento, indican que solo están disponibles como atributos, no hay ningún elemento equivalente.

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor TCPPort genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio TCPPort.

Tabla 147. Elementos de supervisor TCPPort	
Elemento	**Descripción**
$bytesPerSec	Número promedio de bytes transferidos cada segundo.
$bytesTransferred	Número de bytes cargados o descargados.
$connectTime*(ConnectTime)	Tiempo que se tarda en establecer una conexión con el servidor de destino.
$downloadTime*(DownloadTime)	Tiempo que se tarda en descargar datos.
$lastlineThere's	Contenido de la última línea recibida del servidor de destino.
$lookupTime*(LookupTime)	Tiempo que se tarda en obtener la dirección IP del servidor de host.
$networkError	Contiene los errores de red durante la conexión.
$port* (Port)	Puerto del servidor de destino al que ha intentado conectarse el supervisor.
$waitingFor	Si la conexión termina antes de que el supervisor haya completado su secuencia de esperas y envíos, este elemento contiene el contenido de la última propiedad WaitFor.

Mensaje de estado

El supervisor TCPPort proporciona mensajes de estado en el atributo ResultMessage cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado TCPPort.

Tabla 148. Mensajes de estado de supervisor TCPPort	
Mensaje	**Descripción**
Aceptar	La solicitud se ha realizado correctamente.
Tiempo de espera agotado mientras se espera leer/escribir	Se ha establecido una conexión de datos con el servidor, pero no responde.
La conexión se ha cerrado inesperadamente	La conexión con el servidor se ha interrumpido.
Conexión fallida	El supervisor no ha podido conectarse al servidor. Para obtener más información, consulte el archivo de registro.
Error de conexión de red	Hay un problema con la red.
Error de red al leer	

Propiedades

Las opciones de propiedades específicas para el supervisor TCPPort se describen en la tabla siguiente.

Tabla 149. Propiedades TCPPort		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
`Desconexión de supervisor`	`0`|`1`	Especifica que el supervisor se debe desconectar a sí mismo después del último mandato Send o `WaitFor`. Si el último mandato es Send, el supervisor se desconecta inmediatamente después de que se envíe la cadena. Si el último mandato es `WaitFor`, el supervisor se desconecta en cuanto recibe una coincidencia o cuando se supera el tiempo de espera de sondeo. `0` - inhabilitado (el supervisor no se conecta) `1` - habilitado
`OutputDirectory`	serie	Especifica el directorio de salida para utilizar si se guarda `OutputResult`. Valor predeterminado: `$ISHOME/var`.
`OutputResult`	`0`|`1`	Especifica que el supervisor debe guardar los datos que recibe del servicio. `0` - inhabilitado `1` - habilitado
`Send`	*n*	La cadena literal que escribe el supervisor en el puerto. Consulte Directrices para configurar el supervisor TCPPort. n es un número de 1 a 30 inclusive.
`singleLineMatch`	`0`|`1`	Especifica que el supervisor debe devolver una única coincidencia de línea cuando coincide con una expresión regular. `0` - inhabilitado (coinciden varias líneas) `1` - habilitado (coincide una sola línea)
`WaitFor`	*n*	La expresión regular utilizada para coincidir con mandatos o cadenas en el puerto supervisado. Para obtener más información, consulte Directrices para configurar el supervisor TCPPort. n es un número de 1 a 30 inclusive.

Suites de cifrado

La propiedad `SSLCipherSuite` especifica la suite de cifrado utilizada el supervisor TCPPORT. Para más información sobre valores SSL, consulte "Establecimiento de SSL en Internet Service Monitoring" en la página 454.

Supervisor TFTP

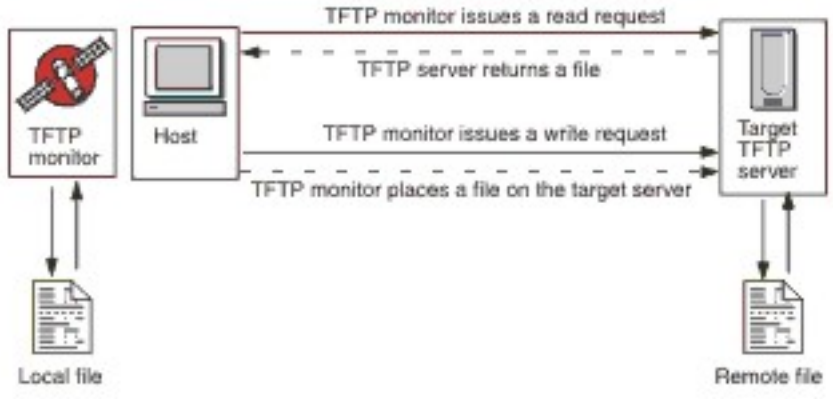
El supervisor TFTP mide el rendimiento del servicio Trivial File Transfer Protocol (TFTP) entre dos sistemas.

En la tabla siguiente se enumeran los archivos de supervisor TFTP.

Tabla 150. Resumen del supervisor FTP	
Archivos de supervisor	**Nombre o ubicación**
Nombre de ejecutable	`nco_m_tftp`
Archivo de propiedades	`$ISHOME/etc/props/tftp.props`
Archivo de reglas	`$ISHOME/etc/rules/tftp.rules`
Archivo de registro	`$ISHOME/log/tftp.log`

Directrices para configurar el supervisor TFTP

El supervisor TFTP transfiere archivos entre el sistema host y el servidor de destino utilizando solicitudes READ o WRITE de TFTP y, a continuación, registra el tiempo de respuesta y la velocidad de transferencia de datos. Utilícelo para asegurarse de que el servidor TFTP está activo y en ejecución, y de que transfiere archivos a una velocidad aceptable.



Para cargar un archivo, el supervisor envía la solicitud TFTP WRITE (WRQ), y para descargar un archivo envía la solicitud TFTP READ (RRQ). En los clientes TFTP, la operación de carga es PUT y la operación de descarga es GET.

El supervisor TFTP admite las modalidades de transferencia de archivos octet (binaria) y netascii.

Configuración de pruebas de servicios de supervisor TFTP

Utilice los parámetros de configuración del supervisor TFTP para definir pruebas de servicios.

Tabla 151. Configuración del supervisor TFTP	
Campo	**Descripción**
server	Dirección IP del servidor TFTP de destino o sistema desde/hacia el que desea transferir archivos.
localfile	Para las operaciones GET, este campo especifica el nombre y la vía de acceso donde se descarga el archivo. Para las operaciones PUT, este campo especifica el nombre y la vía de acceso del archivo que se carga en el servidor.
remotefile	Para las operaciones GET, este campo especifica el nombre y la vía de acceso del archivo que se descarga del servidor. Para las operaciones PUT, este campo especifica el nombre y la vía de acceso donde se carga el archivo al servidor.

Tabla 151. Configuración del supervisor TFTP (continuación)	
Campo	**Descripción**
description	Campo de texto para proporcionar información descriptiva sobre el supervisor TFTP.
port	Puerto que utiliza el servidor TFTP. Valor predeterminado: 69
localip	Dirección IP de la interfaz de red del host en la que el supervisor abre la conexión TFTP. Si este campo está en blanco, el supervisor utiliza la interfaz especificada por la propiedad `IpAddress`.
localport	Puerto que utiliza el supervisor para establecer la conexión TFTP. Si el valor de este campo es `0`, el supervisor selecciona un puerto adecuado.
command	El mandato TFTP que el supervisor debe utilizar: • GET>: descargar un archivo del servidor de destino en el host del supervisor. • PUT: cargar un archivo del host del supervisor en el servidor de destino. Valor predeterminado: GET
transfermode	Especifica el formato en el que el supervisor transfiere el archivo: • OCTET (8 bits) • NETASCII Valor predeterminado: OCTET
timeout	Tiempo de espera, en segundos, para que responda el servidor TFTP. Valor predeterminado: 10
retries	Número de veces que el supervisor intenta transferir un archivo antes de abandonar. Valor predeterminado: 3
poll	Tiempo, en segundos, entre cada sondeo. No establezca este valor en un tiempo demasiado bajo, ya que el sondeo constante podría saturar el servicio. Valor predeterminado: 300
failureretests	Número de veces que el supervisor vuelve a probar el servidor TFTP después de una anomalía inicial antes de que se indique el error. Valor predeterminado: 0

Tabla 151. Configuración del supervisor TFTP (continuación)	
Campo	**Descripción**
retestinterval	El tiempo, en segundos, que se debe esperar entre cada repetición de prueba de anomalía. Valor predeterminado: 10

Clasificaciones de nivel de servicio

Las clasificaciones del nivel de servicio definen las reglas para determinar el nivel de servicio suministrado por un servidor TFTP.

Las opciones de clasificación del nivel de servicio disponibles para el supervisor TFTP son estas:

```
totalTime
lookupTime
responseTime
transferTime
bytesTransferred
bytesPerSec
checksum
message
```

En las clasificaciones del nivel de servicio:

- Especifique más clasificaciones de nivel de servicio entrando manualmente el nombre del elemento supervisor. El nombre debe coincidir con el nombre que se muestra para el elemento en la sección Elementos de supervisor.
- `message` puede ser cualquier mensaje que se reenvíe en el elemento `$message` al servidor IBM Application Performance Management si se utiliza en cualquier widget. Para obtener una lista de valores posibles, consulte Mensajes de estado.
- El operando es una serie o un número positivo.
- El elemento `checksum` no proporciona normalmente resultados significativos para las clasificaciones del nivel de servicio. Su valor es desconocido cuando se crea el elemento de perfil. El supervisor calcula los valores de suma de comprobación durante la realización de las pruebas. Este elemento está pensado para el enriquecimiento de alertas mediante archivos de reglas.

Elementos de supervisor

Además de los resultados de las pruebas comunes para todos los elementos, el supervisor TFTP genera un conjunto de resultados de las pruebas que contienen datos específicos de las pruebas del servicio TFTP.

En la tabla siguiente se describen los elementos adicionales para el supervisor TFTP.

Tabla 152. Elementos del supervisor TFTP	
Elemento	**Descripción**
`$bytesPerSec*` (`BytesPerSec`)	Número promedio de bytes transferidos cada segundo.
`$bytesTransferred*` (`BytesTransferred`)	Número de bytes cargados o descargados.
`$checksum`	Valor de suma de comprobación de los datos descargados. Lo genera el supervisor y se proporciona para el procesamiento adicional mediante archivos de reglas.

Tabla 152. Elementos del supervisor TFTP (continuación)	
Elemento	**Descripción**
$command* (TftpCommand)	Mandato TFTP que emite el supervisor (GET o PUT).
$localFile* (TftpLocalFile)	Nombre de vía de acceso completa del archivo almacenado en el host local. Este elemento se toma del archivo de configuración.
$localIP	Dirección IP local configurada para ser utilizada por el supervisor. Puede estar en blanco en un sistema con una sola interfaz.
$lookupTime* (LookupTime)	Tiempo que se tarda en obtener la dirección IP del servidor de host.
$remoteFile* (TftpRemoteFile)	Nombre de vía de acceso completa del archivo almacenado en el host remoto (el servidor FTP). Este elemento se toma del archivo de configuración.
(TransferTime)	Tiempo que se tarda en transferir el archivo.
(TftpConnection)	Formato en el cual el supervisor transfiere el archivo. Es OCTET (8 bits) o NETASCII.

Mensajes de estado

El supervisor TFTP proporciona mensajes de estado en el atributo ResultMessage cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

Tabla 153. Mensajes de estado del supervisor TFTP	
Mensaje	**Descripción**
OK (CORRECTO)	La solicitud TFTP se ha realizado correctamente.
FAILED: connect failed (FALLO: la conexión ha fallado)	El supervisor no ha podido conectarse al servidor. Compruebe que el servidor se está ejecutando.
FAILED: internal tftp monitor error (FALLO: error interno de supervisor tftp)	Hay un problema con el supervisor, posiblemente causado por insuficiencia de memoria.

Tabla 153. Mensajes de estado del supervisor TFTP (continuación)	
Mensaje	**Descripción**
`FAILED: A send/wait timed out` (FALLO: se ha excedido el tiempo de envío/espera)	Ha fallado la solicitud TFTP. Es posible que haya un problema con la red.
`FAILED: An unspecific error condition. The transfer should be aborted` (FALLO: condición de error no específica. La transferencia se debe cancelar)	
`FAILED: Received a short or malformed packet` (FALLO: se ha recibido un paquete breve o incorrectamente formado)	
`FAILED: local file open/read/write failed` (FALLO: no se ha podido abrir/leer/escribir el archivo local)	
`FAILED: unrecognized status from transfer attempt` (FALLO: estado no reconocido desde intento de transferencia)	

Ejemplo

Pruebe la disponibilidad del servidor TFTP `tftp.mycompany.com` cargando el archivo `$ISHOME/etc/testfiles/upload.txt` en `/ism/test/upload_result.txt`. Utilice la modalidad netascii para cargar el archivo a intervalos de 20 minutos

Clasifique el nivel de servicio según los criterios siguientes:

- Si la carga no se realiza correctamente, el nivel de servicio es `Failed`
- Si el tiempo total de transferencia es superior a 10 segundos, el nivel de servicio es `Marginal`
- De lo contrario, el nivel de servicio es `Good`.

Cree un elemento de perfil de supervisor TFTP y establecer la configuración como se muestra en la tabla siguiente.

Tabla 154. Ejemplo de elemento de perfil TFTP	
Campo de configuración	**Valores**
server	tftp.mycompany.com
localfile	`$ISHOME/etc/ism/testfiles/upload.txt`
remotefile	`/ism/test/upload_result.txt`
description	Prueba TFTP
Active	Seleccionado
command	PUT
transfermode	NETASCII
poll	1200

Tabla 154. Ejemplo de elemento de perfil TFTP (continuación)	
Campo de configuración	**Valores**

statement	`If (Message != OK) then status Failed`
	`else if (TotalTime > 10) then status`
	`Marginal`
	`else status Good`

Supervisor TRANSX

El supervisor TRANSX simula las acciones de un usuario real de internet ejecutando una serie de actividades, que realiza utilizando otros supervisores de servicios de Internet.

Por ejemplo, configure TRANSX para acceder a páginas de un sitio web utilizando el supervisor HTTP, descargar algunos archivos, enviar o recibir correos electrónicos utilizando los supervisores POP3 y SMTP.

En la tabla siguiente se enumeran los archivos de supervisor TRANSX.

Tabla 155. Archivos de supervisor TRANSX	
Archivos de supervisor	**Nombre o ubicación**
Archivo ejecutable de supervisor	`nco_m_transaction`
Archivo de propiedades	`$ISHOME/etc/props/transx.props`
Archivo de reglas	`$ISHOME/etc/rules/transx.rules`
Archivo de registro	`$ISHOME/log/transx.log`

Propiedades

Tabla 156. Propiedades de supervisor TRANSX		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
`CompleteTransax`	`0`|`1`	Especifica que la transacción continúa aunque falle un paso. • `0` - inhabilitado (no continúa) • `1` - habilitado (continúa)
`DetailedTimings`	`0`|`1`	Especifica que el supervisor TRANSX genera registros de datos que contienen temporizaciones ajustadas para cada paso. Las temporizaciones ajustadas generadas en los registros de datos están preestablecidos y no se pueden modificar. • `0` - inhabilitado • `1` - habilitado
`MultipleEvents`	`0`|`1`	Especifica si el supervisor genera varios sucesos para resultados de transacción: • `0` - inhabilitado (el supervisor solo genera un suceso que contiene los resultados de todos los pasos y resultados de resumen) • `1` - habilitado (el supervisor genera un sucesos para cada paso de la transacción y un suceso de resumen final)

Tabla 156. Propiedades de supervisor TRANSX (continuación)		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
StepPause	entero	Especifica la duración de la pausa, en segundos, entre la ejecución de cada paso de transacción. La duración de la pausa no afecta al valor del elemento $totalTime de una transacción. $totalTime representa la suma de elementos $stepXTime de una transacción. Valor predeterminado: 0

En la tabla siguiente se describen las propiedades específicas del supervisor SMTP.

Directrices para configurar el supervisor TRANSX

El supervisor TRANSX prueba servicios simulando un conjunto de actividades que engloban una experiencia de usuario típica. El conjunto de actividades se denomina transacción, y cada actividad de la transacción se denomina paso de transacción.

Los elementos de perfil TRANSX definen las transacciones. Cada paso de transacción configura un supervisor de servicios de Internet como, por ejemplo, HTTP, para realizar la operación para es paso. Configure pasos de transacción a través del botón Editar en la pestaña Pasos del elemento de perfil TRANSX.

Los pasos se configuran de la misma forma que se configura cualquier otro elemento de perfil. Por ejemplo, los detalles de configuración para un paso que implica que el supervisor HTTP puede incluir parámetros de cabecera/formulario, parámetros de servidor de proxy, expresiones regulares y clasificaciones de nivel de servicio.

Cuando el supervisor TRANSX prueba un paso en la transacción, registra el tiempo que se tarda y el nivel de servicio para el paso.

Nota: El supervisor TRANSX requiere privilegios raíz si alguno de los pasos de transacción utiliza otro supervisor como, por ejemplo, ICMP, que requiere privilegios raíz.

Manejo de contenido dinámico con supervisores HTTP y HTTPS

Muchos sitios web utilizan el contenido dinámico para proporcionar funciones como, por ejemplo, interacciones basadas en sesión o en región. Cuando se utiliza junto con el supervisor TRANSX, los supervisores HTTP y HTTPS pueden probar páginas web que contengan contenido dinámico como, por ejemplo, ID de sesión, códigos de región, o fechas y horas incluidas en enlaces, cuyos valores pueden ser diferentes cada vez que se prueba la transacción.

Las características de contenido dinámico proporcionadas por los supervisores HTTP y HTTPS cuando se ejecutan en modalidad de transacción permiten identificar contenido dinámico en forma de pares de nombre-valor, llamados elementos de página dinámicos, que se incluyen en los URL o se definen en los elementos form HTML, que el supervisor extrae de una página durante cada prueba, asegurándose de que se utiliza el valor dinámico apropiado cada vez que se prueba una transacción.

Por ejemplo, suponga una página de inicio de sesión de un sitio web, http://www.mycompany.com/login, que contiene un enlace para el inicio de sesión en el sitio web. El URL de enlace para la acción de inicio de sesión http://www.mycompany.com/doLogin?sessionID=id incluye un ID de sesión para la transacción de inicio de sesión. En este ejemplo, el par de nombre-valor sessionID=id es un elemento de página dinámico; el valor de id cambia cada vez que se accede a la página de inicio de sesión. Para probar la página de inicio de sesión como parte de una transacción, se configuraría la transacción para obtener y utilizar el valor de sessionID cada vez que se prueba la transacción, y para insertarla en la URL de la acción de inicio de sesión.

El supervisor TRANSX pasa elementos de página dinámicos de un paso de transacción a otro. En el ejemplo de inicio de sesión de sitio web, el primer paso de la transacción accedería a la página de

inicio de sesión para obtener el ID de sesión y, después, lo pasa a un segundo paso, que envía la solicitud de inicio de sesión que contiene ese ID. Las operaciones realizadas en estos pasos son:

1. Acceder a la página que contiene los elementos de página dinámicos, por ejemplo, `http://www.mycompany.com/login`
2. Enviar la acción utilizando los elementos de página dinámicos, por ejemplo, `http://www.mycompany.com/doLogin?sessionID=@@030671`

Cuando se identifica un elemento de página dinámico en un paso de transacción, se pasa al siguiente paso de transacción, que inserta el par nombre-valor en su solicitud. El elemento se pasa en cada transacción HTTP o HTTPS posterior, hasta que lo elimina de forma explícita.

Añadir y eliminar páginas dinámicas

Cada paso de transacción HTTP o HTTPS consta de una solicitud, que devuelve una página HTML. Cuando se ejecuta un paso de transacción que contiene elementos de página dinámicos, el monitor analiza la página HTML para localizar el par nombre-valor de cada elemento y lo pasa al siguiente paso de transacción, que los inserta en su solicitud HTTP o HTTPS.

Para especificar que un paso utiliza elementos de página dinámicos, establezca el tipo de parámetro para el elemento en DYNAMIC. A continuación, especifique cada elemento dinámico que se va a extraer y pasar en pasos posteriores. Identifique cada elemento dinámico especificando su nombre, por ejemplo, `sessionID` y seleccione Añadir a como el valor. Añadir a indicia que el elemento se va a pasar en pasos posteriores.

Nota: Para obtener el nombre de un elemento de página dinámico, consulte el origen HTML de la página en la cual se encuentra.

Los elementos de página dinámicos se pasan de un paso de transacción al siguiente. Si deja de ser necesario pasar un elemento de página al siguiente paso, establezca el Valor del elemento en Eliminar de. Actualice manualmente los pasos de transacción posteriores para asegurarse de que se procesan los elementos de página correctos.

Utilice las directrices siguientes para añadir y eliminar elementos de página dinámicos:

- Si un paso no utiliza ningún elemento de página dinámico, no seleccione DYNAMIC como tipo de parámetro.
- Si un paso requiere un elemento de página dinámico, el paso que recupera la página en la cual aparece el elemento dinámico debe especificar el nombre del elemento y el valor Añadir a.
- Si un paso no requiere que se pase un elemento dinámico desde pasos anteriores, establezca el valor del paso anterior en Eliminar de.

GET y POST

En los métodos GET, todos los elementos de página dinámicos se insertan en el URL de la solicitud de forma automática. En los métodos POST, debe especificar cada elemento dinámico como un parámetro FORM en la pestaña Parámetros.

El supervisor inserta automáticamente el valor dinámico para cada formulario cuando ejecuta el paso de transacción.

Creación de una transacción

Defina transacciones creando elementos de perfil TRANSX y pasos de transacción utilizando la interfaz de usuario de Internet Service Monitoring. Para obtener más información, consulte “Creación de transacciones” en la página 454.

Configuración de la prueba de servicios de supervisor TANSX

Tabla 157. Configuración de supervisor TRANSX

Campo	Descripción
transxname	Un nombre para la transacción.

Tabla 157. Configuración de supervisor TRANSX (continuación)	
Campo	**Descripción**
description	Campo de texto para proporcionar información descriptiva sobre el elemento.
poll	El tiempo, en segundos, entre cada sondeo. Valor predeterminado: 300

Nota: Supervise la disponibilidad de un sitio web utilizando una secuencia de navegación web, descargas de archivo y mensajes de correo electrónico enviados.

1. Cree un elemento de perfil TRANSX.
2. Cree un paso de transacción HTTP para supervisar la disponibilidad de un sitio web.
3. Cree un paso de transacción FTP para supervisar una descarga de archivo.
4. Cree un paso de transacción POP3 o SMTP para supervisar el correo electrónico.

Consulte la documentación para cada supervisor para obtener más información.

Elementos de supervisor

El supervisor TRANSX genera sucesos que contienen los resultados de cada transacción. Estos sucesos contienen los resultados de toda la transacción, así como los resultados de los pasos de transacción individuales.

Sin embargo, de forma predeterminada, el supervisor coloca todas las transacciones y los resultados de los pasos en un solo suceso utilizando la propiedad `MultipleEvents`, que puede configurar en el supervisor para crear sucesos individuales para cada paso de transacción y un suceso de resumen para toda la transacción. En la Tabla 1 se enumeran los elementos de resumen TRANSX.

Los elementos indicados con un asterisco (*) están disponibles como atributos. Los nombres de los atributos se muestran entre corchetes. La ausencia de un asterisco indica que no hay ningún atributo equivalente. Los atributos que se muestran entre corchetes, pero sin un elemento indican que solo están disponibles como atributos, no hay ningún elemento equivalente.

Tabla 158. Elementos de supervisor de resumen TRANSX	
Elemento	**Descripción**
`$numberOfSteps*(NumberOfSteps)`	El número de pasos de la transacción.
`$stepDescriptions`	Una lista de las descripciones para cada paso, separadas por un carácter de barra vertical (`|`).
`$stepTimes*(Step`*`1 to 10`*`TotalTime)`	Los datos de tiempo devueltos por cada paso (de 1 a 10).
`$stepUnits`	Una lista de las unidades para cada paso, normalmente, segundos, separadas por un carácter de barra vertical (`|`).
`(TransName)`	El nombre de la transacción como se especifica cuando se configura la transacción.
`(TransStepDescription)`	La descripción del paso de transacción como se especificó al configurar el paso.

Mensaje de estado

El supervisor TRANSX proporciona mensajes de estado en el atributo `ResultMessage` cuando se utiliza IBM Application Performance Management. Estos mensajes indican el resultado de la prueba.

En la tabla siguiente se describen los mensajes de estado.

Tabla 159. Mensajes de estado de supervisor TRANSX	
Mensaje	**Descripción**
`Transacción completada correctamente`	La transacción se ha completado correctamente.
`Error en transacción`	Se ha producido un error en uno de los pasos de la transacción.
`Ha fallado el nivel de servicio, finalizando transacciónHa fallado el nivel de servicio`	El nivel de servicio de uno de los pasos ha devuelto una respuesta fallida, que ha provocado que se detenga la transacción.

Creación de transacciones
Las transacciones se pueden definir creando elementos de perfil TRANSX y pasos de transacciones que utilizan la interfaz de usuario de Agente de Internet Service Monitoring.

Procedimiento

Para crear una transacción mediante la interfaz:

1. Pulse **Icono de configuración del sistema**. Debajo de este icono pulse **Configuración del agente**.
   Se abre la ventana de configuración del agente.
2. Pulse **ISM** para configurar el agente de Internet Service Monitoring.
3. Pulse el icono de suma **(+)** para crear un perfil nuevo. Especifique el **Nombre de perfil** y **Descripción**.
4. Pulse **Siguiente**.
5. Pulse Supervisor **TRANSX** en la lista desplegable de supervisores para seleccionar Supervisor TRANSX.
6. Pulse **Siguiente**.
7. Especifique los parámetros obligatorios.
8. En el separador **Avanzados**, especifique el **intervalo de sondeo**.
9. Pulse el icono de suma **(+)** en el separador Pasos.
10. Pulse el supervisor que necesite seleccionar en la lista desplegable de supervisores.
11. Pulse **Seleccionar** para configurar el paso de transacción.
    a) Especifique los parámetros obligatorios y opcionales de la misma forma que anteriormente para configurar los elementos de perfil.
    b) Si está creando pasos dinámicos para el supervisor HTTP o HTTPS, establezca los pares de Nombre y Valor en el separador Parámetros y seleccione DYNAMIC como el tipo de parámetro.
12. Pulse **Añadir**.
13. Pulse el icono Renovar en la cuadrícula de pasos.
14. Repita los pasos del 1 al 13 para obtener más ayuda sobre la transacción.
15. Pulse **Añadir** para finalizar.
16. Pulse **Hecho** para guardar.

Resultados

Nota: Para especificar una pausa entre cada paso de la transacción, utilice la propiedad `StepPause`.

Establecimiento de SSL en Internet Service Monitoring
Internet Service Monitoring utiliza OpenSSL para comunicarse de forma segura con servicios de Internet normalmente remotos utilizando distintos supervisores, por ejemplo, el supervisor HTTPS se comunica con un HTTPD seguro. Agente de Internet Service Monitoring también utiliza OpenSSL entre los supervisores y Databridge y entre el agente de Agente de Internet Service Monitoring (KIS) y Databridge. Especifique la suite de cifrado que utiliza la aplicación en la propiedad `SSLCipherSuite`.

Databridge se debe configurar para comunicarse de forma segura con los supervisores y Agente de Internet Service Monitoring para que cada supervisor comparta un conjunto común de propiedades relacionadas con Databridge para gestionar la comunicación segura con Databridge. Algunos supervisores también compartan un conjunto similar, pero diferente, de propiedades relacionadas para gestionar la comunicación segura con sus respectivos servicios de Internet bajo prueba.

Los supervisores siguientes admiten la supervisión de servicios de Internet seguros:

- HTTPS
- IMAP4
- POP3
- SMTP

Estos supervisores utilizan certificados. Todos los certificados se almacenan en formato X509 en archivos .Pem (Privacy Enhanced Mail) in `$ISMHOME/certificates`. El certificado para Databridge también se almacena en la misma ubicación. Por este motivo, las propiedades siguientes son compartidas por todos los supervisores, Databridge y Agente de Internet Service Monitoring:

- SSLTrustStore (Valor predeterminado: $ISMHOME/certificates/trust.pem)
- SSLTrustStorePath (Valor predeterminado: $ISMHOME/certificates/)

Como todas la comunicaciones entre supervisores y Databridge, y entre supervisores seleccionados y sus servicios de Internet seguros se basan en la misma versión de OpenSSL, comparten características. Por ejemplo, el nivel más alto de seguridad que puede proporcionar Internet Service Monitoring es una función del nivel más alto proporcionado por el OpenSSL subyacente. El nivel inferior de seguridad proporcionado depende de forma similar del OpenSSL subyacente.

Si el Agente de Internet Service Monitoring se actualiza y esa actualización incluye una actualización en el OpenSSL subyacente, los servicios de Internet que se supervisan pueden verse afectados. Por ejemplo:

1. El supervisor HTTPS en Agente de Internet Service Monitoring V7.x.1 está supervisando un servidor HTTPD protegidos.
2. Aplique una nueva versión de Agente de Internet Service Monitoring que contenga una versión actualizada de OpenSSL, lo que significa que el supervisor HTTPS ahora es V7.x.2.
3. Puede advertir que el supervisor HTTPS ahora no puede supervisar el HTTPD protegido.

El nivel de seguridad del servidor HTTPD es menor que el mínimo soportado por Agente de Internet Service Monitoring V7.x.2 recién actualizado. Aunque la configuración del supervisor HTTPS no ha cambiado, su comportamiento lo ha hecho, porque depende de la capa de OpenSSL subyacente. La combinación más nueva de Agente de Internet Service Monitoring/HTTPS Monitor/OpenSSL es más segura que la combinación antigua y, ahora, tendrá que aumentar el nivel de seguridad del servidor HTTPD remoto.

La supervisión de servicios de Internet protegidos le presenta un dilema. ¿Debería el nivel de seguridad de Agente de Internet Service Monitoring tan bajo que pueda supervisar los servicios de Internet poco protegidos?; o ¿debería ser tan alto como los valores mínimos recomendados actualmente? Si se selecciona el primero, a continuación, un Agente de Internet Service Monitoring debilitado podría comprometer la seguridad, posiblemente, en ambos extremos.

Todos los supervisores deben utilizar la misma versión de OpenSSL. Todos estos supervisores comparten un conjunto común de propiedades de supervisor para configurar el OpenSSL subyacente, que se describen en la tabla siguiente.

Tabla 160. Propiedades de supervisor relacionadas con OpenSSL

Nombre de propiedad	Parámetro de propiedad	Descripción
SSLCipherSuite	serie	Especifica las suites de cifrado que se deben utilizar para operaciones SSL entre el supervisor y el servicio de Internet que está supervisando. Los valores para esta propiedad deben tener el formato recomendado por OpenSSL. Valor predeterminado: AES:3DES:DES:!EXP:!DHE:!EDH
SSLDisableSSLv2	0|1	Determina qué tipo de conexión segura realizar al supervisar un servicio de Internet protegido. 0 – SSLv2 está permitido 1 – SSLv2 NO está permitido Valor predeterminado: 1 (SSLv2 NO permitido).
SSLDisableSSLv3	0|1	Determina qué tipo de conexión segura realizar al supervisar un servicio de Internet protegido. 0 – SSLv3 está permitido 1 – SSLv3 NO está permitido Valor predeterminado: 1 (SSLv3 NO permitido).
SSLDisableTLS	0|1	Determina qué tipo de conexión segura realizar al supervisar un servicio de Internet protegido. 0 – TLSv1.0 está permitido 1 – TLSv1.0 NO está permitido Valor predeterminado: 0 (TLSv1.0 está permitido).
SSLDisableTLS11	0|1	Determina qué tipo de conexión segura realizar al supervisar un servicio de Internet protegido. 0 – TLSv1.1 está permitido 1 – TLSv1.1 NO está permitido Valor predeterminado: 0 (TLSv1.1 está permitido).
SSLDisableTLS12	0|1	Determina qué tipo de conexión segura realizar al supervisar un servicio de Internet protegido. 0 – TLSv1.2 está permitido 1 – TLSv1.2 NO está permitido Valor predeterminado: 0 (TLSv1.2 está permitido).

Tabla 160. Propiedades de supervisor relacionadas con OpenSSL (continuación)

Nombre de propiedad	Parámetro de propiedad	Descripción
SSLCertificateFile	serie	La vía de acceso y el nombre de archivo del certificado digital público utilizado por el supervisor. Cuando un supervisor intenta configurar una conexión protegida con un servicio de Internet, este último puede solicitar, si lo desea, que el supervisor proporcione su certificado del lado del cliente, lo que permite al servicio de Internet verificar el supervisor o el cliente (verificación del certificado del lado del cliente). El certificado debe tener el formato PEM (correo con privacidad mejorada). Para el supervisor HTTPS, este valor se puede especificar para cada elemento HTTPS en el momento de la creación. Sin embargo, si el supervisor HTTPS va a utilizar el mismo certificado para todos los elementos, se utiliza el valor del archivo HTTPS.props. Para supervisores IMAP, LDAP, POP3, SIP, SMTP y SOAP, el valor se establece en el nivel de supervisor. Si la vía de acceso no es absoluta, el supervisor lo interpreta como relativo al directorio de trabajo, $ISMHOME/certificates. Valor predeterminado: “”
SSLKeyFile	serie	La vía de acceso y el nombre de archivo del archivo que contiene la clave privada utilizada por el supervisor. El supervisor utiliza este archivo para cifrar los mensajes que envía a otros. Los receptores utilizan el certificado digital público del supervisor para descifrar el mensaje. Valor predeterminado: monitoryKey.pem
SSLKeyPassword	serie	La contraseña utilizada para cifrar la clave privada SSL. Valor predeterminado: “”

Tabla 160. Propiedades de supervisor relacionadas con OpenSSL (continuación)		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
SSLTrustStoreFile	serie	El nombre completo del archivo que almacena todos los certificados públicos X509 de los servicios de Internet que se están supervisando, como una lista concatenada. Los certificados revocados (CRL) también se almacenan aquí como una lista concatenada. Databridge también puede almacenar aquí su certificado público. Esta propiedad aparece en el archivo `bridge.props`. Los certificados se almacenan en formato PEM (correo con privacidad mejorada). Convierta los certificados obtenidos en otros formatos a formato PEM utilizando el software OpenSSL disponible en http://www.openssl.org. Valor predeterminado: **"$ISMHOME/certificates/trust.pem"**
SSLTrustStorePath	serie	La ubicación de los archivos `.pem` que contienen los certificados X509 del servicio de Internet seguro que se está supervisando. Los certificados revocados (CRL) también se almacenan aquí. Databridge también puede almacenar aquí su certificado público. Esta propiedad aparece en el archivo `bridge.props`. Si se añaden nuevos certificados a este directorio, ejecute el mandato openssl `rehash` para examinar el directorio y calcular un hash para cada certificado. Si se utilizan ambas propiedades, `SSLTrustStoreFile` y `SSLTrustStorePath`, OpenSSL utiliza ambas propiedades para localizar certificados de confianza. Valor predeterminado: "`$ISMHOME/certificates/`"
`VerifyCertificate Preference`	0|1	Habilita o inhabilita la verificación del certificado proporcionado por el servicio de Internet que se está supervisando en relación con la lista de revocación de certificados (CRL). Valor predeterminado: 0 - inhabilitado

Suites de cifrado

Las suites de cifrado disponibles en Internet Service Monitoring son un subconjunto de las suites permitidas por OpenSSL. El conjunto de suites de cifrado permitidas por OpenSSL cambia con el paso del tiempo. A medida que se descubren nuevas vulnerabilidades y evolucionan mejores prácticas, el acceso a tipos específicos o generales de suites de cifrado puede estar restringido o puede haber sido eliminado por completo por OpenSSL. Puesto que estas versiones posteriores de OpenSSL están

incluidas en versiones posteriores de ISM, hay un flujo en vigor que puede afectar a la configuración y el funcionamiento de los supervisores.

Utilice la propiedad de nivel de supervisor SSLCipherSuite para especificar las suites de cifrado permitidas por un supervisor de todas las suites de cifrado disponibles utilizando palabras clave. Para especificar varias suites, utilice una lista separada por dos puntos de palabras clave. Por ejemplo, la propiedad SSLCipherSuite predeterminada es AES:3DES:DES:!EXP:!DHE:!EDH. Esta selección significa que las suites de cifrado que incluyen AES, 3DES y DES están permitidas, pero excluye cualquier suite de cifrado que utilice intercambios de clave EXP (Export (longitudes de clave cortas)), DHE (Diffie Hellman Exchange) o EDH (Ephemeral Diffie Hellman). Además, cuando la conexión segura se realiza entre el supervisor y el servicio de Internet, primero se utiliza AES, seguido por 3DES y, después, DES si es necesario. La sintaxis para las listas de suites de cifrado para Agente de Internet Service Monitoring es la misma que para OpenSSL.

Para seleccionar el conjunto correcto de suites de cifrado para un supervisor, tenga en cuenta lo que admite el OpenSSL subyacente, el rango de cifrados que admite el servicio de Internet que se está supervisando y los estándares de seguridad de la organización. Es posible que no pueda supervisar un sitio externo seguro que tenga un nivel de seguridad inferior al tolerado por Internet Service Monitoring u OpenSSL. En algunos casos, un supervisor que alguna vez pudo supervisar un servicio de Internet, puede fallar después de actualizar Internet Service Monitoring porque los niveles de seguridad son incompatibles.

En la tabla siguiente se lista un subconjunto de suites de cifrado equivalentes al valor predeterminado para SSLCiperSuite de AES:3DES:DES:!EXP:!DHE:!EDH con sus propiedades. En la tabla, verá los términos siguientes:

- Nombre de suite de cifrado: describe la paquete de cifrado que utiliza un nombre construido a partir de palabras clave.
- Protocolo: describe la versión del protocolo soportado.
- Intercambio de claves: describes el sistema de intercambio de claves utilizado para el cifrado y descifrado.
- Cifrado y longitud de clave: describe el tipo de algoritmo de cifrado utilizado y la longitud de la clave (en bits) utilizada.
- MAC: describe el código de autenticación de mensaje utilizado para asegurarse de que los datos no se han alterado.

Tabla 161. Nombre de suite de cifrado y valores de propiedad AES:3DES:DES:!EXP:!DHE:!EDH

Nombre de suite de cifrado	Protocolo	Intercambio de claves	Autenticación	Cifrado y longitud de clave	Código de autenticación de mensaje
ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM(256)	AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES(256)	SHA384
ECDHE-RSA-AES256-SHA	SSLv3	ECDH	RSA	AES(256)	SHA1
ECDHE-ECDSA-AES256-SHA	SSLv3	ECDH	ECDSA	AES(256)	SHA1

Tabla 161. Nombre de suite de cifrado y valores de propiedad AES:3DES:DES:!EXP:!DHE:!EDH (continuación)

Nombre de suite de cifrado	Protocolo	Intercambio de claves	Autenticación	Cifrado y longitud de clave	Código de autenticación de mensaje
SRP-DSS-AES-256-CBC-SHA	SSLv3	SRP	DSS	AES(256)	SHA1
SRP-RSA-AES-256-CBC-SHA	SSLv3	SRP	RSA	AES(256)	SHA1
SRP-AES-256-CBC-SHA	SSLv3	SRP	SRP	AES(256)	SHA1
DH-DSS-AES256-GCM-SHA384	TLSv1.2	DH/DSS	DH	AESGCM(256)	AEAD
...seguido por 61 filas más					

En la tabla siguiente se lista un subconjunto de suites de cifrado equivalente al valor para `SSLCiperSuite` de `AES:3DES:DES:!EXP:!DHE:!EDH:!SSLv2:!SSLv3` con sus propiedades. Ahora, se eliminan algunos protocolos y el conjunto general de suites de cifrado se ha reducido de 71 a 31.

*Tabla 162. Nombre de suite de cifrado y valores de propiedad **AES:3DES:DES:!EXP:!DHE:!EDH:!SSLv2:!SSLv3***

Nombre de suite de cifrado	Protocolo	Intercambio de claves	Autenticación	Cifrado y longitud de clave	Código de autenticación de mensaje
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM(256)	AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES(256)	SHA384
DH-DSS-AES256-GCM-SHA384	TLSv1.2	DH/DSS	DH	AESGCM(256)	AEAD
DH-RSA-AES256-GCM-SHA384	TLSv1.2	DH/RSA	DH	AESGCM(256)	AEAD
DH-RSA-AES256-SHA256	TLSv1.2	DH/RSA	DH	AES(256)	SHA256
DH-DSS-AES256-SHA256	TLSv1.2	DH/DSS	DH	AES(256)	SHA256
ADH-AES256-GCM-SHA384	TLSv1.2	DH	Ninguna	AESGCM(256)	AEAD
ADH-AES256-SHA256	TLSv1.2	DH	Ninguna	AES(256)	SHA256
ECDH-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH/RSA	ECDH	AESGCM(256)	AEAD
...seguido por 21 filas más					

Reducción de la vulnerabilidad

En releases futuros, los cifrados DHE y EDH estarán inhabilitados de forma predeterminada debido a las vulnerabilidades. Para versiones anteriores de Agente de Internet Service Monitoring, es posible que tenga que inhabilitar los cifrados DHE y EDH en todos los supervisores. Para inhabilitar los

cifrados DHE y EDH, actualice las propiedades de supervisor `SSLCipherSuite` y `BridgeSSLCipherSet`.

Por ejemplo, para inhabilitar los cifrados DHE y EDH en el supervisor HTTPS, actualice el archivo `https.props` para incluir las propiedades siguientes:

```
SSLCipherSuite: AES:3DES:DES:!DES-CBC-SHA:!EXP:!DHE:!EDH
BridgeSSLCipherSet: AES:3DES:DES:!DES-CBC-SHA:!EXP:!DHE:!ED
```

Asegúrese de verificar que este cambio de configuración no provoca ningún problema de compatibilidad. Si cambia el valor predeterminado después de aplicar este arreglo, puede exponerse usted mismo a una vulnerabilidad de seguridad. Debería revisar todo el entorno completo para identificar otras áreas en las que ha habilitado el protocolo de intercambio de claves Diffie-Hellman utilizado en TLS y realizar acciones de mitigación y reparación.

Selección de protocolo

Puede seleccionar entre una gama de protocolos de comunicación seguros históricos y actuales. Se pueden seleccionar de forma individual utilizando un conjunto de propiedades de supervisor booleanas:

- SSLDisableSSLv2
- SSLDisableSSLv3
- SSLDisableTLS
- SSLDisableTLS11
- SSLDisableTLS12
- BridgeSSLDisableSSLv2
- BridgeSSLDisableSSLv3

Debe inhabilitar SSLv2 y SSLv3. Estos protocolos se han visto comprometidos y tienen varias vulnerabilidades conocidas. Están inhabilitadas de forma predeterminada y solo se proporcionan para fines de legado.

De forma predeterminada Internet Service Monitoring admite TLS. Si sabe que los servicios de Internet que está supervisando no utilizan TLS 1.0 y ya se han aumentado a TLS 1.1 o TLS 1.2, deberá inhabilitar los protocolos no utilizados en Internet Service Monitoring.

El componente Databridge se comunica con el agente de Internet Service Monitoring y con cada uno de los supervisores. De forma predeterminada, esta comunicación está cifrada y TLS es el protocolo preferido.

Almacenes de confianza de clave y certificados

Internet Service Monitoring almacena sus certificados en un archivo definido por usuario en una ubicación definida por usuario. Todos los certificados se deben almacenar en formato PEM (correo con privacidad mejorada). Asegúrese de que los certificados públicos obtenidos de otras organizaciones se convierten a formato PEM. El software de conversión está disponible en http://www.openssl.org.

Los certificados de confianza especificados utilizando la propiedad `SSLTrustStoreFile` se almacenan en el archivo como una lista concatenada.

Es una buena práctica almacenar las listas de revocación de certificados (CRL) en el almacén de confianza con el que se pueden validar los certificados. Las entidades emisoras de certificados tienen sistemas en vigor para generar listas de certificados revocados y tienen sistemas de distribución aplicados para hacerlos disponibles públicamente. A continuación, si se compromete un certificado, se revocará.

Valores de seguridad de Databridge

Todos los supervisores se comunican con Databridge, así que los supervisores tienen un conjunto común de propiedades que se deben establecer para gestionar la comunicación entre los supervisores y Databridge. De forma predeterminada, la comunicación está cifrada. El protocolo de

cifrado predeterminado es TLS. A diferencia de las propiedades de supervisor, no hay ningún mecanismo para controlar si una versión concreta de TLS está habilitada o inhabilitada. Todos los supervisores deben tener los mismos valores para las propiedades Databridge, de lo contrario, habrá problemas de comunicación. De forma similar, las propiedades establecidas en el archivo .props de Databridge deben ser coherentes con las propiedades de los supervisores. Databridge también se comunica con el agente de Internet Service Monitoring que tiene su propio archivo .props. Algunos de los valores del .props del agente están relacionados con supervisores Databridge y similares deben tener valores que sean coherentes con los valores del archivo `.props` de Databridge.

Tabla 163. Propiedades Databridge relacionadas con OpenSSL

Nombre de propiedad	Parámetro de propiedad	Descripción
BridgeSSLEncryption	0|1	Determina si la comunicación con Databridge está cifrada o no. Esto cubre toda la comunicación de Databridge con supervisores y el agente de Internet Service Monitoring. `0` – no cifrado `1` – cifrado **Restricción:** Establezca el mismo valor en el agente de Internet Service Monitoring, todos los supervisores y Databridge.
BridgeSSLCipherSet	serie	Especifica las suites de cifrado que se deben utilizar para operaciones de SSL a y desde Databridge. Los valores para esta propiedad deben tener el formato recomendado por OpenSSL. **Restricción:** Establezca el mismo valor en el agente de Internet Service Monitoring, el agente, todos los supervisores y Databridge. Valor predeterminado: `AES:3DES:DES:!EXP:!DHE:!EDH`
BridgeSSLDisableSSLv2	0|1	Determina qué tipo de conexión segura realizar a y desde Databridge. `0` – SSLv2 y SSLv3 están permitidos `1` – SSLv2 NO está permitido **Restricción:** Establezca el mismo valor en el agente de Internet Service Monitoring, todos los supervisores y Databridge. Valor predeterminado: 1 (SSLv2 NO permitido).
BridgeSSLDisableSSLv3	0|1	Determina qué tipo de conexión segura realizar a y desde Databridge. `0` – SSLv3 está permitido `1` – SSLv3 NO está permitido **Restricción:** Establezca el mismo valor en el agente de Internet Service Monitoring, todos los supervisores y Databridge. Valor predeterminado: 1 (SSLv3 NO permitido).

Tabla 163. Propiedades Databridge relacionadas con OpenSSL (continuación)

Nombre de propiedad	Parámetro de propiedad	Descripción
BridgeSSLCertificateFile	serie	La vía de acceso y el nombre de archivo del certificado SSL de Databridge digital. Valor predeterminado: `$ISMHOME/certificates/bridgeCert.pem`
BridgeSSLKeyFile	serie	La vía de acceso y el nombre de archivo del archivo de claves privadas SSL de Databridge. Valor predeterminado: `$ISMHOME/certificates/bridgeKey.pem`
BridgeSSLKeyPassword	serie	La contraseña utilizada para cifrar la clave privada SSL de Databridge. Valor predeterminado: **Tivoli**
BridgeSSLTrustStore	serie	La vía de acceso y el nombre de archivo del archivo de certificado de confianza para la autenticación. Esto solo es necesario cuando se utiliza la propiedad **BridgeSSLAuthenticatePeer**. Valor predeterminado: `$ISMHOME/certificates/trust.pem` Si desea configurar la autenticación SSL entre un supervisor y Databridge, o entre Databridge y el agente, establezca `BridgeSSLAuthenticatePeer` en 1 y reinicie Databridge. Esta acción autentica los certificados del servidor. Puede almacenar certificados tanto en `SSLTrustStoreFile`, como `SSLTrustStorePath`. Valores predeterminados: • `SSLTrustStoreFile`, `$ISMHOME/certificates/trust.pem` • `SSLTrustStorePath`, `$ISMHOME/certificates/` Para añadir nuevos certificados, realice uno de los pasos siguientes: • Añada un certificado al final de la lista en el archivo de texto `SSLTrustStoreFile` • Añada un nuevo certificado al directorio `SSLTrustStorePath` y ejecute el mandato OpenSSL **c_rehash certificate_dir** para realizar hash en los certificados
SSLTrustStoreFile	serie	Esta propiedad es utilizada por supervisores seguros y Databridge. Consulte Tabla 160 en la página 456 para obtener más información.
SSLTrustStorePath	serie	Esta propiedad es utilizada por supervisores seguros y Databridge. Consulte Tabla 160 en la página 456 para obtener más información.

Tabla 163. Propiedades Databridge relacionadas con OpenSSL (continuación)		
Nombre de propiedad	**Parámetro de propiedad**	**Descripción**
BridgeSSLAuthenticatePeer	0|1	Especifica si Databridge se debe autenticar de forma cruzada con otros componentes de Internet Service Monitoring. 0 – inhabilitado 1 – habilitado Si un supervisor se pone en contacto con Databridge, debe autenticarse con Databridge, y Databridge debe autenticarse con el supervisor. Si el agente de Internet Service Monitoring se pone en contacto con Databridge, se debe autenticar con Databridge, y Databridge se debe autenticar con el agente. Los certificados para Databridge se almacenan en BridgeSSLTrustStore. Valor predeterminado: 0 - inhabilitado

Propiedades de agente de Internet Service Monitoring

Agente de Internet Service Monitoring tiene su propio archivo de propiedades, que contiene un conjunto de propiedades y valores de seguridad. El archivo de propiedades de agente no se comunica con los supervisores, pero se comunica con Databridge, de forma que los valores del archivo `.props` del agente gestionan la comunicación entre el agente y Databridge.

Configuración del agente en sistemas Windows

Puede configurar el agente en sistemas Windows utilizando la ventana de **IBM Performance Management**.

Procedimiento

Configure el agente de Agente de Internet Service Monitoring en el sistema del usuario de la forma siguiente.

Para configurar manualmente el agente de Internet Service Monitoring en los sistemas del usuario:

1. En el **panel de instrumentos de IBM Performance Management**, pulse **Configuración del sistema** > **Configuración del agente** que aparece bajo **Configuración del sistema**.
2. Pulse **ISM** para abrir el panel de instrumentos del agente de Internet Service Monitoring.

Configuración de Databridge

La configuración de Databridge implica establecer propiedades para el Databridge que controlan su funcionamiento como, por ejemplo, la conexión de los módulos de componentes y los supervisores de servicios de Internet.

Funcionamiento y configuración
Databridge y sus módulos de componente se configuran a través de archivos de propiedades.

Las propiedades determinan el funcionamiento de Databridge y sus módulos de componente que envían resultados de prueba a IBM Cloud Application Performance Management para informar sobre el panel de instrumentos del agente de Internet Service Monitoring.

Configuración de Databridge
Databridge se debe configurar para recibir datos de los supervisores de servicios de Internet y para reenviar estos datos a sus módulos de componente para su posterior proceso.

En la tabla siguiente se muestran los archivos asociados con Databridge. **`Archivo de propiedades`**, **`Archivo de almacenamiento y reenvío`** y **`Archivo de registro`** se describen más detalladamente en las secciones pertinentes.

Tabla 164. Archivos de Databridge y su ubicación

Archivo de Databridge	**Ubicación o nombre**
Archivo ejecutable	`$ISHOME/platform/arch/bin/nco_m_bridge`
Archivo de propiedades	`$ISHOME/etc/props/bridge.props`
Archivo de almacenamiento y reenvío	El nombre y la ubicación se especifican mediante propiedades del archivo `bridge.props`. El nombre y ubicación predeterminado es `$ISHOME/var/sm_bridge.saf`
Archivo de registro	`$ISHOME/log/bridge.log`
Archivo de registro de errores	`$ISHOME/log/bridge.err`

Archivo SAF (Almacén y reenvío)
Si Databridge no puede reenviar datos a Netcool/OMNIbus, almacena todos los datos que enviaría en circunstancias normales en un archivo SAF (Almacén y reenvío). Cuando Netcool/OMNIbus vuelve a estar disponible, procesa todos los sucesos almacenados en el archivo SAF.

Las propiedades QFile y QSize del archivo de propiedades de Databridge determinan el nombre, la ubicación y el funcionamiento del proceso de almacén y reenvío.

Archivo de registro
El Databridge envía mensajes diariamente sobre sus operaciones en un archivo de registro de mensajes. De forma predeterminada, el nombre de este archivo es `$ISHOME/log/bridge.log`. Se actualiza a las 12 de la medianoche. Las propiedades de Databridge MsgDailyLog y MsgTimeLog controlar el funcionamiento del registro de mensajes.

Inicio de Databridge
Inicio de Databridge utilizando la consola de servicios de Windows.

Procedimiento

Nota: Si el módulo ObjectServer está conectado a Databridge, asegúrese de que su sistema de destino se está ejecutando antes de iniciar Databridge. Si alguno de los módulos Databridge no se puede inicializar correctamente, Databridge no se iniciará.

1. En el escritorio de Windows, pulse **Iniciar** > **Herramientas administrativas** > **Servicios**.
2. En la lista de servicios, seleccione el servicio denominado NCO BRIDGE Internet Service Monitor y pulse **Iniciar** en el menú.

Conexión de módulos
El archivo de propiedades de Databridge define los módulos para conectar a Databridge.

Acerca de esta tarea
Cada par de propiedad de Module n `SharedLib` y Module n `PropFile` define la conexión para un módulo. Los módulos se cargan en orden de definición, empezando por Module0.

Procedimiento

1. Para conectar módulos individuales a Databridge:

a) En el archivo de propiedades de Databridge, identifique el siguiente par disponible de propiedad Module n `SharedLib` y Module n `PropFile`.

b) Establezca Module n `SharedLib` en el nombre de la biblioteca compartida del módulo (su implementación binaria).

c) Establezca Module n `PropFile` en la vía de acceso completa del archivo de propiedades del módulo.

En este ejemplo, las líneas 1 y 2 conectan el módulo ObjectServer, las líneas 3 y 4 conectan el módulo Datalog, las líneas 5 y 6 conectan el módulo IBM Application Performance Management (`pipe`). El módulo Datalog no tiene un archivo de propiedades, por lo que la entrada para el archivo de propiedades tiene el valor `""`.

2. Para inhabilitar un módulo:

a) Establezca la propiedad Module n `SharedLib` en `"NONE"` y la propiedad Module n `PropFile` en `""`. Todos los demás módulos que tienen un valor superior a n también se ignoran.

Conexión de supervisores
Los supervisores de servicios de Internet se conectan a Databridge a través de TCP. Cada supervisor tiene un conjunto de propiedades que configura la conexión a Databridge.

Acerca de esta tarea
Para conectar un supervisor a Databridge, establezca el valor de la propiedad `BridgePort` definida en el archivo de propiedades del supervisor en el valor de la propiedad `SocketPort` definida en el archivo de propiedades de Databridge. El valor predeterminado de la propiedad `BridgePort` de cada supervisor y la propiedad `SocketPort` del Databridge es `9510`.

El databridge admite el cifrado SSL de los resultados de prueba que recibe de los supervisores. Para cifrar los resultados de prueba de un supervisor, establezca los valores de las propiedades `BridgeSSL` definidas en el archivo de propiedades del supervisor en los valores de las propiedades `BridgeSSL` definidas en el archivo de propiedades de Databridge. Para cifrar todos los resultados de prueba de los supervisores, todos los supervisores deben tener las mismas propiedades `BridgeSSL`.

Configuración del módulo Databridge
Databridge direcciona los resultados de pruebas al agente de Internet Service Monitoring. El agente de supervisión convierte estos datos al formato necesario y los distribuye al servidor IBM Application Performance Management. Configure el módulo Databridge y el agente de supervisión de servicios de Internet a través de sus archivos de propiedades respectivos.

Configure la operación de Databridge modificando los valores de propiedad definidos en el archivo de propiedades del módulo.

El archivo de propiedades del módulo se denomina `pipe_module.props`. Este archivo se encuentra en el directorio `$ISHOME/etc/props/`.

La siguiente tabla lista las propiedades disponibles para el módulo. Si se realizan cambios en las propiedades, reinicie Databridge para que estos cambios entren en vigor.

Tabla 165. Propiedades del módulo Databridge

Nombre de propiedad	Tipo	Descripción
TEMAHOST	serie	El nombre del host que ejecuta el agente de supervisión. Valor predeterminado: `localhost`
TEMAPORT	entero	El número de puerto utilizado por el host. Valor predeterminado: `9520`

Configure el funcionamiento del agente de supervisión de servicios de Internet modificando los valores de propiedades en el archivo de propiedades del agente de supervisión.

El archivo de propiedades del agente de supervisión se llama `kisagent.props`. Este archivo se encuentra en el directorio `$ISMHOME/etc/props/`.

La siguiente tabla lista las propiedades disponibles para el agente de supervisión.

Tabla 166. Propiedades de agente supervisión

Nombre de propiedad	Tipo	Descripción
TEMAPORT	entero	El número de puerto utilizado por el host. Este número debe ser el mismo que el número de puerto para la propiedad TEMAPORT listada en el archivo de propiedades de módulo. Valor predeterminado: 9520
ObsoleteDuration	entero	El tiempo, en segundos, después del cual se borran los datos que no se han actualizado de la memoria del agente de supervisión. Por ejemplo, puede que los datos no se hayan actualizado cuando un elemento de perfil se ha detenido o cuando se ha producido un error de red. **Nota:** No establezca el tiempo de ObsoleteDuration en un valor menor que el intervalo de sondeo porque esto provoca una pérdida de datos entre los intervalos de sondeo. Valor predeterminado: 900
AggDuration	entero	El tiempo, en segundos, después del cual el agente de supervisión deja de agregar a y notificar datos en el panel de instrumentos del agente. Los datos más antiguos que el tiempo especificado se suprimen de la memoria del agente de supervisión. Los datos antiguos se calculan comparando el intervalo entre la hora de inicio y la hora actual con el tiempo de duración global. Si el intervalo es mayor que el tiempo de duración global, se elimina un 10 por ciento de los datos antiguos y la hora de inicio se aumenta en una décima parte del intervalo. El agente de supervisión lo calcula cada 5 minutos. Valor predeterminado: 3600
ManageServices	0|1	Inicia y detiene todos los supervisores y Databridge cuando se inicia o se detiene el agente de Internet Service Monitoring. 1 está habilitado y 0 está inhabilitado. Valor predeterminado: 1

La conexión entre el agente de supervisión de servicios de Internet y el módulo de Databridge se crea cuando se instala Internet Service Monitoring.

Habilitación de Netcool/OMNIbus

Siga estos pasos para habilitar Tivoli Netcool/OMNIbus para enviar los sucesos del Agente de Internet Service Monitoring a Netcool/OMNIbus.

Antes de empezar
Asegúrese de que ha instalado IBM Tivoli Netcool/OMNIbus.

Procedimiento

Complete los pasos siguientes para habilitar Netcool/OMNIbus:

1. Detenga el Agente de Internet Service Monitoring mediante el mandato siguiente:

```
$CANDLEHOME/bin/ism-agent.sh stop
```

2. Abra el archivo `bridge.props` ubicado en la vía de acceso `$ISMHOME/etc/props` y actualice el archivo con el siguiente fragmento de código:

```
Module0SharedLib : "libSMModulePipe"
Module0PropFile : "$ISMHOME/etc/props/pipe_module.props"
Module1SharedLib : "libSMModuleObjectServer"
Module1PropFile : "$ISMHOME/etc/props/objectserver.props"
```

3. Modifique el permiso del directorio `8.1.0` ubicado en la vía de acceso `$ISMHOME/objectserver` de la forma siguiente:

```
cd  $ISMHOME/objectserver/
chmod -R 777 8.1.0
```

   Nota: Modifique el permiso de todos los archivos del directorio `8.1.0` utilizando el mandato `chmod -R 777 <nombre-archivo>`. Donde `<nombre-archivo>` es el nombre del archivo dentro del directorio `8.1.0`.

4. Modifique el archivo `omni.dat` que se encuentra en la vía de acceso `$ISMHOME/objectserver/8.1.0/etc` para configurar la dirección del servidor de Netcool/OMNIbus.
5. Ejecute `nco_igen` desde la ubicación siguiente:

```
cd $ISMHOME/objectserver/8.1.0/bin
./nco_igen
```

6. Inicie el Agente de Internet Service Monitoring utilizando el mandato siguiente:

```
$CANDLEHOME/bin/ism-agent.sh start
```

7. Verifique que el Agente de Internet Service Monitoring, Databridge y todos los supervisores estén en estado de ejecución.

   Para comprobar el estado de Databridge y los supervisores, ejecute el mandato siguiente:

```
ps -aef|grep -i nco_*
```

   Para comprobar el estado del Agente de Internet Service Monitoring, ejecute el mandato siguiente:

```
ps -aef|grep -i kis
```

8. Utilice la interfaz de usuario de IBM Tivoli Netcool/OMNIbus para verificar que Databridge envía los datos al servidor de Netcool/OMNIbus.

   Los datos se deben visualizar para el Agente de Internet Service Monitoring en la interfaz de usuario de IBM Application Performance Management.

Configuración de la supervisión de J2SE

Para recopilar datos de supervisión de recursos y diagnóstico de las aplicaciones Java locales que se están supervisando, debe configurar el recopilador de datos J2SE.

Antes de empezar

Instale uno de los tiempos de ejecución Java soportados:

- Oracle Java Platform Standard Edition 7 (Java SE Development Kit 7)

  Recuerde: este tiempo de ejecución Java no da soporte a la imagen del recopilador de datos de J2SE que se configura con el protocolo HTTPS.
- Oracle Java Platform Standard Edition 7 (Java SE Runtime Environment 7)

  Recuerde: este tiempo de ejecución Java no da soporte a la imagen del recopilador de datos de J2SE que se configura con el protocolo HTTPS.
- Oracle Java Platform Standard Edition 8 (Java SE Development Kit 8)
- Oracle Java Platform Standard Edition 8 (Java SE Runtime Environment 8)
- IBM SDK, Java Technology Edition, Versión 7
- IBM SDK, Java Technology Edition, Versión 8

Importante: Para Windows Server 2016, instale JDK 8, Actualización 131 (Java SE Development Kit 8u131) o Java SE Development Kit 7, Actualización 80 (JDK 7u80).

Para obtener más información sobre los requisitos del sistema, consulte Software Product Compatibility Reports for J2SE data collector.

Acerca de esta tarea

Puede configurar el recopilador de datos de J2SE en sistemas Windows, Linux y AIX.

Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agentes y recopiladores de datos y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Procedimiento

1. Copie los archivos siguientes del instalador de APM en un directorio:

   Importante: La vía de acceso del directorio no debe contener espacios.

   - Windows Copie el archivo `gdc.zip` del instalador de APM en un directorio y extráigalo.
   - Linux AIX Copie el archivo `gdc-apd.tar.gz` del instalador de APM en un directorio y extráigalo.
   - Linux AIX Proporcione al usuario permisos de lectura/grabación y ejecución para la carpeta `j2se_dc`. Se proporciona permiso de ejecución para ejecutar scripts y archivos JAR en la carpeta. Se proporciona permiso de lectura/grabación, ya que los archivos de diagnóstico detallado se generan en esta carpeta.
2. En la línea de mandatos, vaya a *DCHOME*`\.gdc\<versión_kit_herramientas>\bin`
   Donde *versión_kit_herramientas* es,
   - Para V8.1.4.0 y versiones anteriores, *versión_kit_herramientas* es 7.3.0.5.0.
   - Para V8.1.4.0.1 y versiones posteriores, *versión_kit_herramientas* es 7.3.0.14.0.
3. Ejecute el mandato siguiente:

   Windows `config.bat`
   Linux AIX `config.sh`
4. Cuando se le solicite, especifique la vía de acceso a Java Home y pulse **Intro**.
   Por ejemplo,

   Windows `C:\Archivos de programa\jre7`
   Linux AIX `/opt/ibm/java`
5. Realice los pasos siguientes según la versión de agente que utilice:
   - Para V8.1.4.0.2 y versiones anteriores, siga estos pasos:

a. Cuando se le solicite, especifique el nombre completo (nombre calificado) de la clase principal de la aplicación y pulse **Intro**. La clase principal es el punto de entrada de la aplicación que se debe supervisar.Ejemplo: `testapp.TemperatureConveter`

b. Cuando se le solicite, especifique un nombre de alias de aplicación distinto y pulse **Intro**. El nombre que especifica aquí se utiliza para crear el nombre de instancia en el panel de instrumentos de APM.

Windows El archivo `dcstartup.bat` se genera en la ubicación siguiente: *DCHOME*`\.gdc\`*versión_kit_herramientas*`\runtime\j2se`*alias_aplicación.nombre_host.alias_aplicación*. Este archivo es el script para ejecutar la aplicación conjuntamente con el recopilador de datos.

Linux AIX El archivo `dcstartup.sh` se genera en la ubicación siguiente: *DCHOME*`/.gdc/`*versión_kit_herramientas*`/runtime/j2se`*alias_aplicación.nombre_host.alias_aplicación*. Este archivo es el script para ejecutar la aplicación conjuntamente con el recopilador de datos.

- Para V8.1.4.0.3 a V8.1.4.0.5, complete los siguientes pasos

a. Cuando se le solicite, especifique el directorio de inicio de la aplicación Java. Por ejemplo, `/root/J2seApp/`

b. Seleccione una aplicación Java de la lista que se proporciona y pulse Salir.

- `com.ibm.SampleApplication`
- `com.ibm.DBApplication`
- `com.ibm.SpringBootApplication`

Seleccione cualquier aplicación que aparezca en la lista o especifique 0 para seleccionar cualquier otra aplicación que no aparezca en la lista.

1) Si especifica 0, especifique el `nombre completo` de la clase Main de cualquier otra aplicación. Por ejemplo, `com.ibm.testApp.Main`

2) Si selecciona cualquier opción de la lista proporcionada, se crea un nombre de alias en función del nombre de clase. Si el nombre de alias sobrepasa el límite de caracteres, proporcione un nombre de alias que esté dentro del límite de caracteres.

Importante: El límite de caracteres máximo para el nombre de alias se calcula de forma tal que `nombre_alias + nombre_host` no supere los 24 caracteres.

c. Seleccione la opción para habilitar o inhabilitar el Rastreo de transacciones. El valor predeterminado es *Sí*.

d. Seleccione la opción para habilitar o inhabilitar la recopilación de datos de diagnóstico. El valor predeterminado es *Sí*.

1) Si selecciona *Sí*, seleccione la opción para la modalidad de Rastreo de métodos. El valor predeterminado es *No*.

e. Si selecciona una opción en la lista que se proporciona en el paso b, copie el script de inicio `<DCHOME>/j2se_dc/.gdc/`*versión_kit_herramientas*`/runtime/j2se<alias_aplicación>.<nombre_host>.<alias_aplicación>` en la ubicación que desee.

- Para V8.1.4.0.6 y posterior, realice los siguientes pasos:

a. Cuando se le solicite, especifique el directorio de inicio de la aplicación Java. Por ejemplo, `/root/J2seApp/`

b. Seleccione el tipo de aplicación que desea supervisar.

- Aplicación Java
- Servidor Jetty

c. Si selecciona el tipo de aplicación *Aplicación Java*, siga los pasos indicados en la sección V8.1.4.0.3 a V8.1.4.0.5 del paso 5.

d. Si selecciona el tipo de aplicación como *Servidor Jetty*, siga estos pasos:

1) Especifique el directorio de inicio de Jetty. Por ejemplo, `/home/jetty/jetty-distribution-9.4.12.v20180830`

2) Escriba el nombre de alias. Si el nombre de alias sobrepasa el límite de caracteres, proporcione un nombre de alias que esté dentro del límite de caracteres.

Importante: Si selecciona el tipo de aplicación *Aplicación Java* y cualquier opción en la lista del paso b de la sección V8.1.4.0.3 a V8.1.4.0.5, copie el script de inicio <DCHOME>/`j2se_dc/.gdc/toolkit_version/runtime/j2se<alias_aplicación>.<nombre_host>.<alias_aplicación>` en la ubicación que desee.

e. Si el tipo seleccionado es *Servidor Jetty*, `dcstartup.bat/dcstartup.sh` se copiará en el directorio de inicio de Jetty dado.

- Para V8.1.4.0.7, siga estos pasos:
  - Si configura el recopilador de datos de J2SE utilizando Open JDK versión 9 o posterior y al especificar la vía de acceso a Java Home se visualiza un aviso con el contenido siguiente:

Aviso:

```
AVISO: Se ha producido una operación de acceso reflexivo no permitida
AVISO: Acceso reflexivo no permitido por parte de jnr.posix.JavaLibCHelper
(archivo:/root/testopen/preconf-13march/j2se_dc/.gdc/7.3.0.14.0/
bin/lib/jython.jar) al método sun.nio.ch.SelChImpl.getFD()
AVISO: Considere la posibilidad de informar de esto a los mantenedores de
jnr.posix.JavaLibCHelper
AVISO: Utilice --illegal-access=warn para habilitar los avisos de las próximas
operaciones de acceso reflexivo no permitidas
AVISO: Todas las operaciones de acceso no permitidas se denegarán en el siguiente
release Mar 15, 2019 11:35:06 AM
org.python.netty.util.internal.PlatformDependent <clinit>
INFO: La plataforma no proporciona una API de bajo nivel completa para
el acceso a almacenamientos intermedios directos de forma fiable. A
menos que se solicite explícitamente, el almacenamiento intermedio dinámico
siempre es preferible para evitar la inestabilidad potencial del sistema.
```

Sin embargo, el recopilador de datos de J2SE funciona correctamente y puede ignorar el aviso.

Para V8.1.4.0.2 y versiones anteriores, siga el paso 6 para modificar el archivo Windows `dcstartup.bat` o Linux AIX `dcstartup.sh`.

6. Para modificar el archivo Windows `dcstartup.bat` o Linux AIX `dcstartup.sh`, siga estos pasos:

- Si las clases de la aplicación y los archivos JAR están empaquetados en un solo archivo JAR, siga estos pasos:

a. Abra el archivo siguiente:

– Windows `dcstartup.bat`

– Linux AIX `dcstartup.sh`

b. Sustituya `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS` *`nombre completo de la clase principal`* por `$ITCAM_JVM_OPTS -jar` *`archivo jar de aplicación`* y guarde el archivo.

- Si la aplicación utiliza varios archivos JAR, siga estos pasos:

a. Abra el archivo siguiente:

– Windows `dcstartup.bat`

– Linux AIX `dcstartup.sh`

b. Establezca la variable *CLASSPATH* en los archivos JAR.

c. Sustituya `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS` *`nombre completo de la clase principal`* por `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS -jar` *`archivo jar de aplicación`* y guarde el archivo.

   El archivo JAR de la aplicación debe contener la clase de aplicación principal.

Nota: Para modificar el archivo Windows `dcstartup.bat` o Linux AIX `dcstartup.sh` para V8.1.4.0.3 en V8.1.4.0.5 y V8.1.4.0.6 a versiones posteriores (si el tipo de aplicación se selecciona como *Aplicación Java*), siga el paso 7.

7. Siga estos pasos si la aplicación utiliza varios archivos JAR.
   a) Abra el archivo siguiente:
      - Windows `dcstartup.bat`
      - Linux AIX `dcstartup.sh`
   b) Establezca la variable *CLASSPATH* en los archivos JAR.
   c) En la V8.1.4.0.7, si configura el recopilador de datos de J2SE con Java 9 o 10 y utiliza la conexión SSL para la conectividad de APM, los datos de Rastreo de transacciones no se visualizarán. Para resolver el problema, puede añadir el distintivo **-- add-modules java.xml.bind** a la última línea del archivo `dcstartup.bat` o `dcstartup.sh`.

      Por ejemplo,

      - Si la aplicación es un archivo jar, actualice la última línea de la forma siguiente:

```
PathToJava --add-modules java.xml.bind --add-opens=

jdk.management/com.sun.management.internal=

ALL-UNNAMED -jar $Classpath $ITCAM_JVM_OPTS AppJarName.jar
```

      - Si la aplicación no está empaquetada en un archivo jar, actualice la última línea de la forma siguiente:

```
PathToJava --add-modules java.xml.bind --add-opens=

jdk.management/com.sun.management.internal=ALL-UNNAMED -cp
.:$classpath:$Classpath $ITCAM_JVM_OPTS FullyQualifiedClassName
```

8. Para habilitar la supervisión de diagnósticos detallados, edite el archivo `custom_request.xml` con las clases y métodos específicos de J2SE que desee supervisar. Puede hacerlo de dos maneras: proceso manual y automático.

   Para llenar automáticamente el archivo `custom_request.xml` con las clases y métodos específicos de la aplicación J2SE:
   a) Vaya al directorio `<DCHOME>/j2se_dc/.gdc/7.3.0.14.0/runtime/j2se<alias_aplicación>.<nombre_host>.<alias_aplicación>/` y abra el archivo `dc.properties`.
   b) Habilite la propiedad `is.auto.update.custom_requests.xml` estableciendo su valor en *true* y guarde el archivo.
   c) Ejecute los mandatos del paso 9.
   d) Detenga el recopilador de datos después de 10 a 15 minutos.
   e) Compruebe que el archivo `DCHOME>/j2se_dc/.gdc/7.3.0.14.0/runtime/j2se<alias_aplicación>.<nombre_host>.<alias_aplicación>/custom/custom_requests.xml` se haya llenado con los métodos y clases personalizados.
   f) Elimine las entradas no deseadas y abra de nuevo el archivo `dc.properties`.
   g) Inhabilite la propiedad `is.auto.update.custom_requests.xml` estableciendo su valor en *false* y guarde el archivo.
   h) Ejecute los mandatos del paso 9.

Nota: Si algunos de los métodos personalizados de la aplicación no se descubren automáticamente, deberá añadirlos manualmente.

Para llenar manualmente el archivo `custom_request.xml`:

a) Vaya a `<DCHOME>/j2se_dc/.gdc/7.3.0.14.0/runtime/j2se<alias_aplicación>.<nombre_host>.<alias_aplicación>/custom/custom_requests.xml` y edite el archivo `custom_request.xml`.

Por ejemplo,

```
<edgeRequest>
<requestName>truncateDb</requestName>
<Matches>testApp.JDBC.DBManager</Matches>
<type>application</type>
<methodName>truncateDb</methodName>
</edgeRequest>
```

b) Añada las clases y métodos específicos de la aplicación.

9. Ejecute el mandato siguiente:

Windows `dcstartup.bat`

Linux AIX `dcstartup.sh`

Nota: Si el tipo de aplicación seleccionado es *Servidor Jetty*, ejecute `dcstartup.bat/dcstartup.sh` presente en el directorio de inicio de Jetty.

La aplicación J2SE se inicia conjuntamente con el recopilador de datos configurado.

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el recopilador de datos en los paneles de instrumentos. Para obtener información sobre cómo utilizar la consola, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Comprobación del estado del rastreo de transacciones y la recopilación de datos de diagnóstico

Para V8.1.0.3 y versiones posteriores, en la página de configuración de agente, puede comprobar el estado del rastreo de transacciones y los datos de diagnóstico.

Acerca de esta tarea

Puede comprobar el estado del rastreo de transacciones y la recopilación de datos de diagnóstico con la ayuda de dos mandatos. Consulte el procedimiento correspondiente para obtener información acerca de estos mandatos.

Procedimiento

1. Utilice el mandato **`config status`**.

a) Abra el directorio bin. Emita el mandato

Linux AIX **`cd <DCHOME>/j2se_dc/.gdc/versión_kit_herramientas/bin/`**

Windows **`cd <DCHOME>\j2se_dc\.gdc\versión_kit_herramientas\bin\`**

Donde *versión_kit_herramientas* es,

- Para V8.1.4.0 y versiones anteriores, *versión_kit_herramientas* es 7.3.0.5.0.
- Para V8.1.4.0.1 y versiones posteriores, *versión_kit_herramientas* es 7.3.0.14.0.

b) Especifique el mandato siguiente para comprobar el estado

Linux AIX **config.sh status**

Windows **config.bat status**

c) Seleccione las aplicaciones identificadas Java con el nombre de alias en la lista para comprobar su estado o seleccione exit.

1) ddperf
2) Main
3) Exit

2. Utilice el mandato **config status <nombre_alias_aplicación>**.

a) Especifique el mandato siguiente para abrir un directorio

Linux AIX **cd <DCHOME>/j2se_dc/.gdc/7.3.0.14.0/bin/**

Windows **cd <DCHOME>\j2se_dc\.gdc\7.3.0.14.0\bin**

b) Especifique el mandato siguiente para comprobar el estado

Linux AIX **config.sh status <nombre_alias_aplicación>**

Windows **config.bat status <nombre_alias_aplicación>**

Cambio del estado del rastreo de transacciones y la recopilación de datos de diagnóstico

Para V8.1.0.3 y versiones posteriores, en la página de configuración de agente, puede cambiar el estado del rastreo de transacciones y los datos de diagnóstico.

Acerca de esta tarea

Puede cambiar el estado del rastreo de transacciones y la recopilación de datos de diagnóstico con la ayuda del indicador de mandatos. Consulte el procedimiento siguiente para obtener información acerca de estos mandatos.

Procedimiento

1. Abra el directorio bin y ejecute el mandato siguiente:

   Linux AIX **cd <DCHOME>/j2se_dc/.gdc/versión_kit_herramientas/bin/**

   Windows **cd <DCHOME>\j2se_dc\.gdc\versión_kit_herramientas\bin**

   Donde *versión_kit_herramientas* es,

   - Para V8.1.4.0 y versiones anteriores, *versión_kit_herramientas* es 7.3.0.5.0.
   - Para V8.1.4.0.1 y versiones posteriores, *versión_kit_herramientas* es 7.3.0.14.0.

2. Para comprobar el estado, especifique el mandato siguiente:

   Linux AIX **config.sh <nombre_alias_aplicación>**

   Windows **config.bat <nombre_alias_aplicación>**

3. Cuando se le solicite, seleccione la opción para habilitar o inhabilitar el Rastreo de transacciones. El valor predeterminado es Sí.
4. Cuando se le solicite, seleccione la opción para habilitar o inhabilitar la recopilación de datos de diagnóstico. El valor predeterminado es Sí.

   a) En caso de seleccionar Sí, seleccione a continuación la opción para habilitar/inhabilitar el Rastreo de método. El valor predeterminado es NO.

Configuración de la supervisión de JBoss

Monitoring Agent for JBoss supervisa los recursos de los servidores de aplicaciones de JBoss y la plataforma JBoss Enterprise Application. Utilice los paneles de instrumentos proporcionados con el agente de JBoss para identificar las aplicaciones más lentas, las solicitudes más lentas, los cuellos de botella de agrupaciones de hebras, problemas de recogida de basura y memoria de almacenamiento dinámico de JVM, las sesiones más ocupadas y otros cuellos de botella del servidor de aplicaciones JBoss.

Antes de empezar

- Las instrucciones siguientes son para el release más reciente del agente, a excepción de lo indicado.
- Asegúrese de que los requisitos del sistema del Agente de JBoss se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de JBoss.
- Antes de configurar el Agente de JBoss, debe configurarse el servidor JBoss completando las tareas siguientes.
  1. "Habilitar las conexiones de servidor de MBean JMX" en la página 477.
  2. "Añadir un usuario de gestión de servidor JBoss" en la página 478.
  3. "Habilitación de la recopilación de estadísticas Web/HTTP" en la página 479. Este procedimiento es para JBoss EAP versión 7.x y WildFly versiones 8.x, 9.x y 10.x.

Acerca de esta tarea

El Nombre de sistema gestionado incluye el nombre de instancia que especifique, por ejemplo, *nombre_instancia*`:`*nombre_host*`:`*pc*, donde *pc* es el código de producto de dos caracteres. El Nombre de sistema gestionado está limitado a 32 caracteres.

El nombre de instancia que especifique está limitado a 28 caracteres menos la longitud del nombre de host. Por ejemplo, si especifica `JBoss` como nombre de instancia, el nombre del sistema gestionado es `JBoss:hostname:JE`.

Nota: Si especifica un nombre de instancia largo, el Nombre de sistema gestionado queda truncado y el código de agente no se visualiza correctamente.

El Agente de JBoss es un agente de varias instancias. Debe crear una instancia de agente para cada servidor JBoss que supervise e iniciar manualmente cada instancia de agente.

La prestación de rastreo de transacciones está disponible para el Agente de JBoss en la oferta Cloud APM, Advanced.

- Para habilitar el rastreo de transacciones para una instancia de agente nueva, complete el paso 1 o el paso 2 de este procedimiento y, a continuación, siga el procedimiento para "Configurar el recopilador de datos de rastreo de transacciones del Agente de JBoss" en la página 486.
- Para habilitar el rastreo de transacciones para una instancia de agente que ya esté configurada para la supervisión básica, siga el procedimiento para "Configurar el recopilador de datos de rastreo de transacciones del Agente de JBoss" en la página 486.
- Para inhabilitar el rastreo de transacciones para una instancia de agente, siga el procedimiento para "Inhabilitar el recopilador de datos de rastreo de transacciones del Agente de JBoss" en la página 488.
- Para desinstalar el rastreo de transacciones para todas las instancias de agente y eliminar el kit de herramientas de rastreo de transacciones, siga el procedimiento para "Desinstalar todo el rastreo de transacciones de Agente de JBoss" en la página 489.

Procedimiento

1. Configure el agente en sistemas Windows mediante la ventana **IBM Performance Management** o el archivo de respuestas silencioso.

- "Configuración del agente en sistemas Windows" en la página 480.
- "Configuración del agente mediante el archivo de respuestas silencioso" en la página 483.

2. Configure el agente en sistemas Linux ejecutando un script de línea de mandatos y respondiendo a las solicitudes, o utilizando el archivo de respuestas silencioso.
   - "Configuración del agente respondiendo a solicitudes" en la página 482.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 483.
3. Opcional: Configure el rastreo de transacciones configurando instancias de agente individuales para proporcionar datos de rastreo de transacciones y configurando el Panel de instrumentos del rendimiento de aplicaciones para visualizar datos de rastreo de transacciones.
   a) Siga el procedimiento para "Configurar el recopilador de datos de rastreo de transacciones del Agente de JBoss" en la página 486.
   b) Habilite los datos de rastreo de transacciones en Panel de instrumentos del rendimiento de aplicaciones para el Agente de JBoss.
      1) En la barra de navegación, pulse **Configuración del sistema** > **Configuración del agente**.Se mostrará la página **Configuración del agente**.
      2) Seleccione la pestaña **JBoss**.
      3) Seleccione los recuadros de selección correspondientes a las instancias de agente del servidor JBoss que desea supervisar y lleve a cabo una de las acciones siguientes de la lista **Acciones**:
         - Para habilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Habilitado**. El estado de la columna **Rastreo de transacciones** se actualizará a *Habilitado*.
         - Para inhabilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Inhabilitado**. El estado de la columna **Rastreo de transacciones** se actualiza a *Inhabilitado*.
   c) Visualice los paneles de instrumentos de datos de rastreo de transacciones del Agente de JBoss añadiendo la instancia del Agente de JBoss a una aplicación en el Panel de instrumentos del rendimiento de aplicaciones.

      Para obtener más información sobre el uso del editor de aplicaciones, consulte Gestión de aplicaciones.
   d) Asegúrese de que las cuentas de usuario están asignadas a un rol que incluya el permiso de panel de instrumentos de diagnóstico para tener acceso a los siguientes botones del Panel de instrumentos de aplicaciones para el rastreo de transacciones del Agente de JBoss.
      De lo contrario, estos botones están inhabilitados para ese usuario en el Panel de instrumentos de aplicaciones.
      1) El botón detallado **Diagnosticar** del widget **5 Tiempos de respuesta más lentos**.
      2) El botón **Solicitudes en curso** del widget **Aplicaciones**.

   Nota: La prestación de rastreo de transacciones está disponible para el Agente de JBoss en la oferta Cloud APM, Advanced. Para el Agente de JBoss con prestación de supervisión de recursos básica, que se encuentra en la oferta Cloud APM, Base, omita este paso.

Qué hacer a continuación

En la Consola de Cloud APM, vaya al Panel de instrumentos del rendimiento de aplicaciones para ver los datos que se han recopilado. Para obtener más información sobre la utilización de la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si no puede ver los datos en los paneles de instrumentos del agente, consulte primero los registros de conexión del servidor y, a continuación, los registros del proveedor de datos. Las vías de acceso predeterminadas a estos registros son las siguientes.

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Si desea recibir ayuda con la resolución de problemas, consulte el Foro de Cloud Application Performance Management.

Habilitar las conexiones de servidor de MBean JMX

Para que el Agente de JBoss pueda recopilar datos del servidor JBoss, deben habilitarse las conexiones del servidor de MBean de Java Management Extensions (JMX).

Procedimiento

Siga los pasos correspondientes a su release y versión del servidor JBoss.

- Configure EAP 5.2.

  Haga una copia de seguridad del archivo `run.conf` y añádale las líneas siguientes:

  ```
  JAVA_OPTS="$JAVA_OPTS -Djboss.platform.mbeanserver"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.ssl=false"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.authenticate=false"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=1090"
  JAVA_OPTS="$JAVA_OPTS -Djavax.management.builder.initial=
                        org.jboss.system.server.jmx.MBeanServerBuilderImpl"
  ```

- Configure AS 6.x.

  Especifique la dirección de enlace como parámetro cuando inicie el servidor JBoss.

  – Linux *inicio_servidor_jboss*`/bin/run.sh` **-b** `dirección_Ip`

  – Windows *nombre_servidor_jboss*`\bin\run.bat` **-b** `<dirección_IP>`

  Donde *inicio_servidor_jboss* es el directorio de instalación del servidor JBoss.

  Por ejemplo, si la dirección de enlace es 10.77.9.250:

  `/apps/wildfly-9.0.2.Final/bin/run.sh` **-b** `10.77.9.250`

- Configure todas las demás versiones soportadas.

  Los servidores JBoss y WildFly se instalan con sus puertos JMX inhabilitados para la gestión remota de forma predeterminada. Debe cambiar la configuración del servidor JBoss para permitir la gestión remota. Debe editar *inicio_servidor_jboss*`/standalone/configuration/standalone.xml` para permitir la gestión remota.

  a) Haga una copia de seguridad del archivo *inicio_servidor_jboss*`/standalone/configuration/standalone.xml`.

  Donde *inicio_servidor_jboss* es el directorio de instalación del servidor JBoss.

  b) Habilite la configuración remota.

  Busque `urn:jboss:domain:jmx` y dentro de la sección del subsistema, asegúrese de que la entrada `remoting-connector` tenga `use-management-endpoint="true"`.

  Resultado de ejemplo.

  ```
  <subsystem xmlns="urn:jboss:domain:jmx:1.3">
              <expose-resolved-model/>
              <expose-expression-model/>
              <remoting-connector use-management-endpoint="true"/>
  </subsystem>
  ```

  c) Habilite las conexiones remotas.

  Busque dónde se definen las interfaces y sustituya 127.0.0.1 (bucle de retorno) por la dirección IP externa en el servidor al que debe enlazarse. No enlace a 0.0.0.0.

  Ejemplo antes de la sustitución.

  ```
    <interfaces>
          <interface name="management">
  ```

```
            <inet-address value="${jboss.bind.address.management:127.0.0.1}"/>
        </interface>
        <interface name="public">
            <inet-address value="${jboss.bind.address:127.0.0.1}"/>
        </interface>
...
```

Ejemplo después de la sustitución si la dirección IP externa es 192.168.101.1.

```
<interfaces>
        <interface name="management">
            <inet-address value="${jboss.bind.address.management:192.168.101.1}"/>
        </interface>
        <interface name="public">
            <inet-address value="${jboss.bind.address:192.168.101.1}"/>
        </interface>
...
```

Añadir un usuario de gestión de servidor JBoss

Para que el Agente de JBoss pueda recopilar datos del servidor JBoss, debe añadirse un usuario de gestión si no existe uno.

Procedimiento

Utilice el script de JBoss **add-user** para añadir un usuario de gestión.

1. Vaya al directorio binario o `bin` bajo el directorio de instalación del servidor JBoss.
2. Ejecute el script **add-user**.
   - Linux **./add-user.sh**
   - Windows **add-user.bat**
3. Siga las solicitudes para generar un usuario de gestión.

Ejemplo

```
root@jboss-wf10-rh7:/apps/wildfly-10.0.0.Final/bin
] ./add-user.sh

¿Qué tipo de usuario que desea añadir?
 a) Usuario de gestión (mgmt-users.properties)
 b) Usuario de aplicación (application-users.properties)
(a): a

Especifique los detalles del nuevo usuario que debe añadirse.
Utilizando el reino 'ManagementRealm' descubierto en los archivos de propiedades existentes.
Nombre de usuario : MyAdmin
Estas son las recomendaciones de contraseña. Para modificar estas restricciones, edite el
archivo de
configuración add-user.properties.
 - La contraseña debe ser diferente del nombre de usuario
 - La contraseña no debe ser uno de los siguientes valores restringidos {root, admin,
administrator}
 - La contraseña debe contener como mínimo 8 caracteres, 1 carácter alfabético, 1 dígito,
1 símbolo alfanumérico
Contraseña:
Vuelva a escribir la contraseña:
¿A qué grupos debe pertenecer este usuario? (Especifique una lista separada por comas, o déjelo
en blanco para ninguno)[  ]:
Se va a añadir el usuario 'MyAdmin' para el reino 'ManagementRealm'
¿Es esto correcto sí/no? sí
Añadido usuario 'MyAdmin' a archivo '/apps/wildfly-10.0.0.Final/standalone/configuration/mgmt-
users.properties'
Añadido usuario 'MyAdmin' a archivo '/apps/wildfly-10.0.0.Final/domain/configuration/mgmt-
users.properties'
Añadido usuario 'MyAdmin' con grupos al archivo
          '/apps/wildfly-10.0.0.Final/standalone/configuration/mgmt-groups.properties'
Añadido usuario 'MyAdmin' con grupos al archivo
          '/apps/wildfly-10.0.0.Final/domain/configuration/mgmt-groups.properties'
¿Va a utilizarse este nuevo usuario para un proceso de AS para conectarse a otro proceso de AS?
Por ejemplo, para que un controlador de host esclavo se conecte con el maestro o para una
conexión
```

```
remota del servidor a llamadas EJB del servidor.
¿sí/no? no
```

Habilitación de la recopilación de estadísticas Web/HTTP

Para que el Agente de JBoss pueda recopilar métricas web del servidor JBoss y otras métricas del subsistema, la recopilación de estadísticas debe estar habilitada para cada subsistema. Este procedimiento es para JBoss EAP versión 7.x y WildFly versiones 8.x, 9.x y 10.x.

Procedimiento

El atributo **statistics-enabled** de varios subsistemas de JBoss controla la recopilación de estadísticas. Este valor se puede ver y actualizar mediante la interfaz de línea de mandatos de JBoss.

Nota: Este procedimiento es para JBoss EAP versión 7.x y WildFly versiones 8.x, 9.x y 10.x.

1. Vaya al directorio binario o `bin` bajo el directorio de instalación del servidor JBoss.
2. Inicie la interfaz de línea de mandatos de JBoss.
   - Linux **./jboss-cli.sh --connect** [**--controller**=*IP*:*puerto*]
   - Windows **jboss-cli.bat --connect** [**--controller**=*IP*:*puerto*]

   donde *IP* es la dirección IP del servidor JBoss y *puerto* es el puerto del servidor JBoss. Por ejemplo, `192.168.10.20:9990`.

   Consejo: Si el intento de conexión genera el error "`Imposible conectarse al controlador: el controlador no está disponible en localhost:9990: java.net.ConnectException: WFLYPRT0053: No se ha podido establecer conexión con http-remoting://localhost:9990. La conexión ha fallado: WFLYPRT0053: No se ha podido establecer conexión con http-remoting://localhost:9990. La conexión ha fallado: conexión rechazada`", utilice el parámetro **--controller**.

   Este error indica que el servidor de gestión no está a la escucha en la dirección IP de localhost (127.0.0.1) y está configurado para escuchar en la dirección IP del sistema.
3. Ejecute los mandatos siguientes para ver el estado actual del atributo statistics-enabled de cada subsistema:

   Nota: Si JBoss se ejecuta en modalidad de dominio, cada mandato debe tener como prefijo el perfil asociado, y estos mandatos deben ejecutarse para cada perfil supervisado. Por ejemplo: `/profile=full/subsystem=ejb3:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`ejb3`**`:read-attribute(name=enable-statistics)`

   `/subsystem=`**`transactions`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`undertow`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`webservices`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`Nombre_origen_datos`*`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`Nombre_origen_datos`*`/`**`statistics=pool`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`Nombre_origen_datos`*`/`**`statistics=jdbc`**`:read-attribute(name=statistics-enabled)`

   donde *Nombre_origen_datos* es el nombre de un origen de datos que se ha configurado para utilizarlo con JBoss.

   Nota: los orígenes de datos pueden listarse mediante el mandato `/subsystem=datasources:read-resource`.

   Ejemplo de resultado cuando las estadísticas no están habilitadas:

```
{
    "outcome" => "success",
    "result" => false
}
```

4. Ejecute el mandato siguiente para cambiar el valor del atributo statistics-enabled de cada subsistema a *true*:

   `/subsystem=`**`ejb3`**`:write-attribute(name=enable-statistics, value=true)`

   `/subsystem=`**`transactions`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`undertow`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`webservices`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`datasources/data-source`**`=`*`Nombre_origen_datos`*`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`datasources/data-source`**`=`*`Nombre_origen_datos`*`/`**`statistics=pool`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`datasources/data-source`**`=`*`Nombre_origen_datos`*`/`**`statistics=jdbc`**`:write-attribute(name=statistics-enabled,value=true)`

   Ejemplo de resultado cuando se habilitan las estadísticas para un subsistema:

```
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
```

5. Salga de la interfaz de línea de mandatos de JBoss.
6. Reinicie el servidor JBoss.

   Nota: Es necesario reiniciar cualquier agente JBoss con rastreo de transacciones que se esté ejecutando actualmente.

Configuración del agente en sistemas Windows

Puede configurar el Agente de JBoss en sistemas operativos Windows utilizando la ventana de IBM Cloud Application Performance Management. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la plantilla **Monitoring Agent for JBoss** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar una instancia de agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar la instancia de agente de nuevo, púlsela con el botón derecho del ratón y luego pulse **Reconfigurar**.
3. Especifique un nombre de instancia exclusivo y luego pulse **Aceptar**. Utilice solamente letras, números, el carácter de subrayado y el carácter menos en el nombre de la instancia.
   Por ejemplo, `jboss01`.

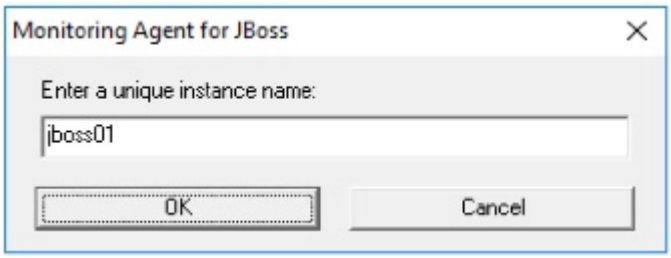


Figura 17. La ventana para especificar un nombre de instancia exclusivo.

4. Especifique los valores del servidor JBoss y, a continuación, pulse **Siguiente**.
   Consulte la sección Tabla 167 en la página 485 para obtener una descripción de cada uno de los parámetros de configuración.

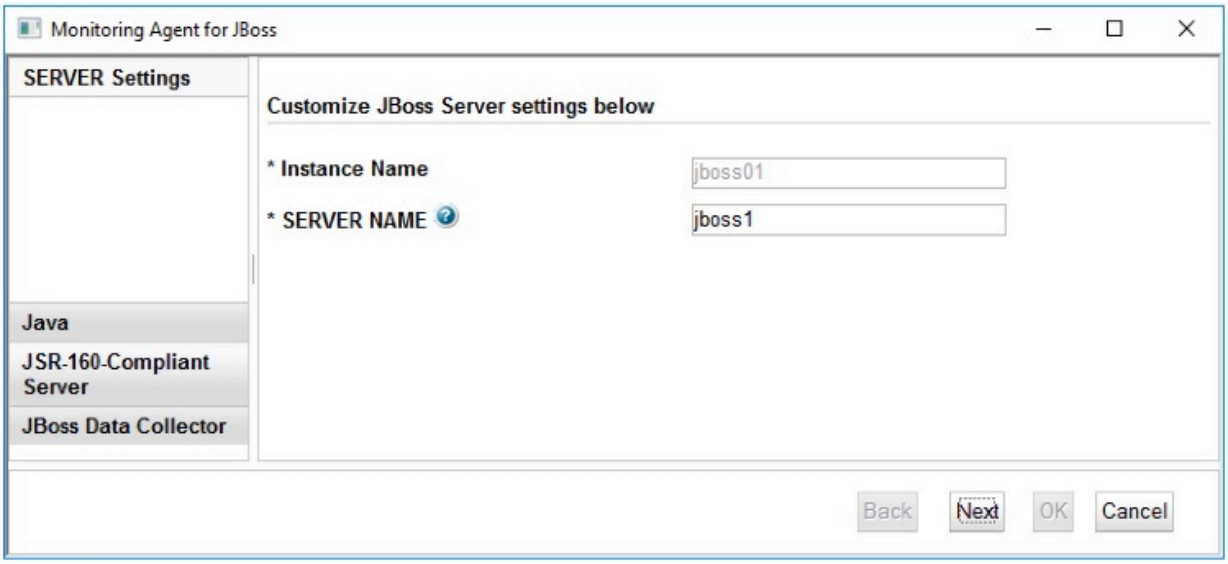


Figura 18. La ventana de los parámetros de configuración del servidor JBoss

5. Especifique los valores de Java y, a continuación, pulse **Siguiente**.
   Consulte la sección Tabla 167 en la página 485 para obtener una descripción de cada uno de los parámetros de configuración.

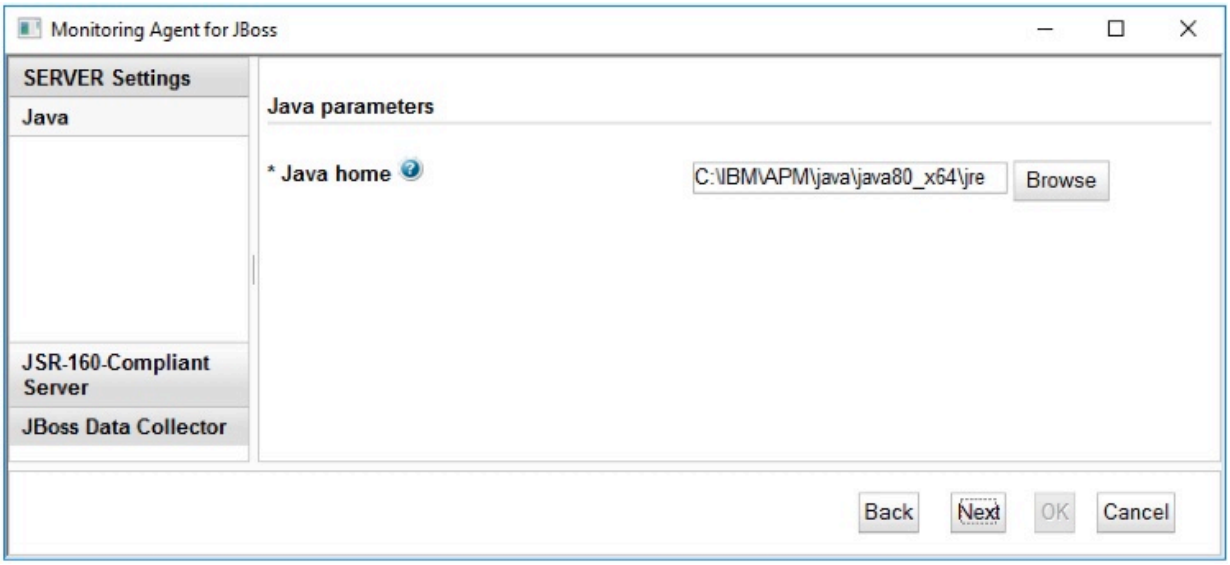


Figura 19. La ventana para especificar valores de Java.

6. Especifique los valores de JMX y pulse **Siguiente**.

Consulte la sección Tabla 167 en la página 485 para obtener una descripción de cada uno de los parámetros de configuración.

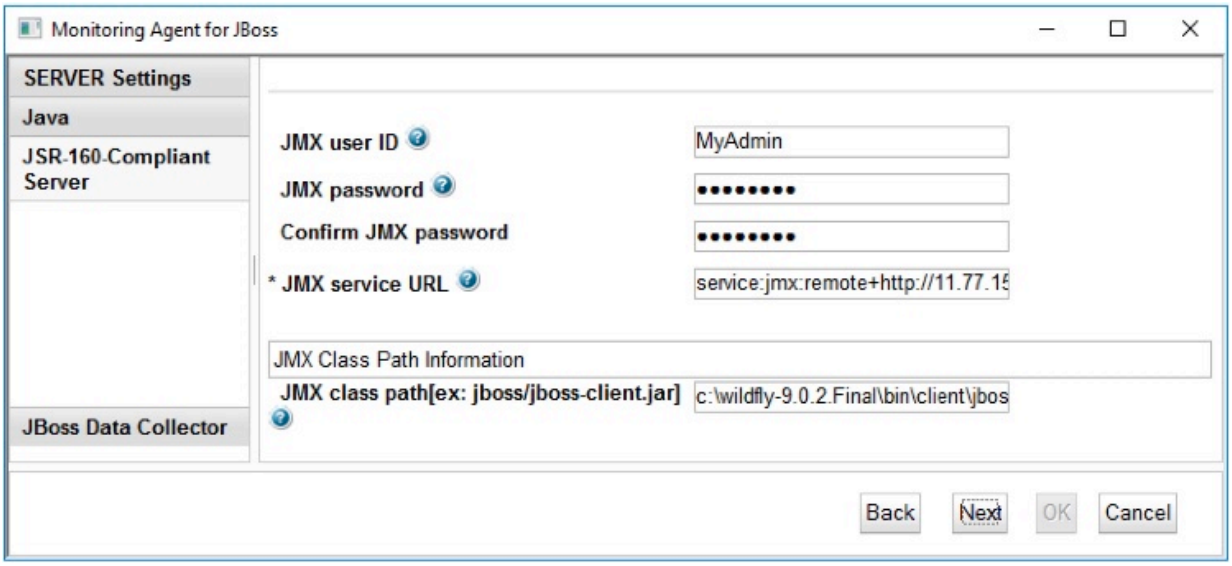


Figura 20. La ventana para especificar valores de JMX.

7. Visualice los valores del recopilador de datos del agente de JBoss.

   Deje en blanco el parámetro **Directorio de tiempo de ejecución de DC** durante la configuración inicial del agente. Consulte la sección Tabla 167 en la página 485 para obtener una descripción de cada uno de los parámetros de configuración.

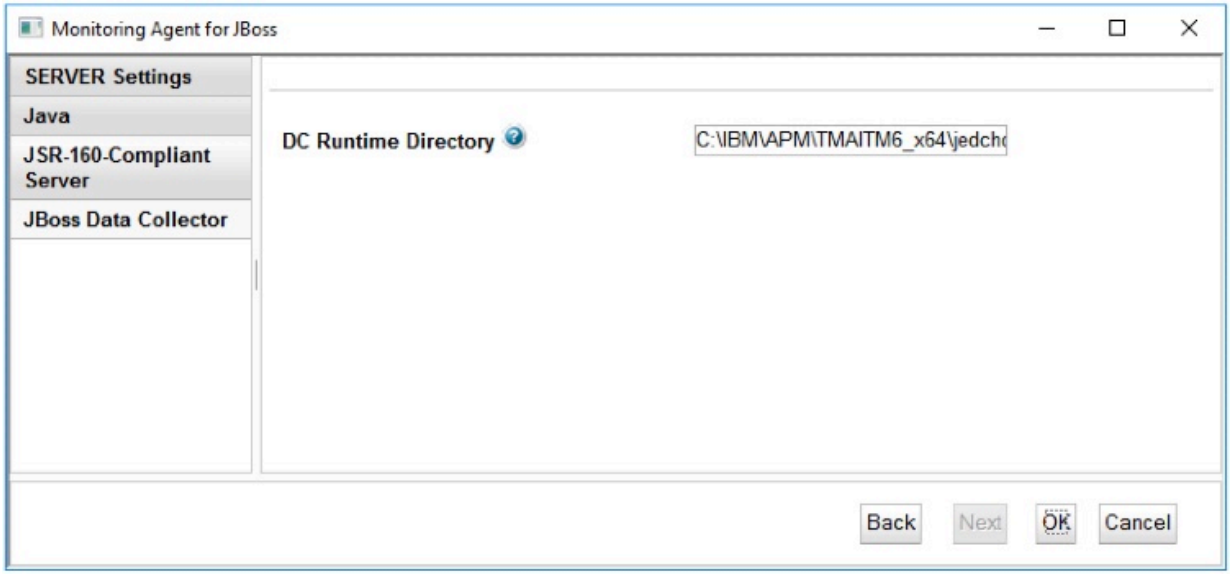


Figura 21. La ventana para especificar los valores del recopilador de datos del agente de JBoss

8. Pulse **Aceptar** para completar la configuración del agente.
9. En la ventana IBM Cloud Application Performance Management, pulse con el botón derecho sobre la instancia que ha configurado y pulse **Iniciar**.

Configuración del agente respondiendo a solicitudes

Después de la instalación del Agente de JBoss, debe configurarlo para poder iniciar el agente. Si el Agente de JBoss está instalado en un sistema Linux o UNIX local, puede seguir estas instrucciones para configurarlo interactivamente a través de solicitudes de línea de mandatos.

Acerca de esta tarea

Recuerde: Si está volviendo a configurar una instancia de agente configurada, se visualiza el valor que se establece en la última configuración para cada opción. Si desea borrar un valor existente, pulse la tecla de espacio cuando se visualice el valor.

Procedimiento

1. En la línea de mandatos, ejecute el mandato siguiente:

   ```
   dir_instalación/bin/jboss-agent.sh config nombre_instancia
   ```

   donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/jboss-agent.sh config example-inst01
   ```

2. Responda a las solicitudes para establecer valores de configuración para el agente.

   Consulte la sección "Parámetros de configuración para el Agente de JBoss" en la página 485 para obtener una descripción de cada uno de los parámetros de configuración.

3. Ejecute el mandato siguiente para iniciar el agente:

   ```
   dir_instalación/bin/jboss-agent.sh start nombre_instancia
   ```

   Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/jboss-agent.sh start example-inst01
   ```

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

- Para configurar el Agente de JBoss en modalidad silenciosa, realice los pasos siguientes:
  a) En un editor de texto, abra el archivo `jboss_silent_config.txt` que está disponible en la siguiente vía de acceso:
     – Linux AIX *dir_instalación*`/samples/jboss_silent_config.txt`

     Ejemplo, `/opt/ibm/apm/agent/samples/jboss_silent_config.txt`
     – Windows *dir_instalación*`\samples\jboss_silent_config.txt`

     Donde *dir_instalación* es la vía de acceso donde está instalado el agente.

Las vías de acceso de *dir_instalación* predeterminadas se listan aquí:

– Linux `/opt/ibm/apm/agent`

– Windows `C:\IBM\APM\TMAITM6_x64`

Ejemplo

Linux AIX
```
/opt/ibm/apm/agent/samples/jboss_silent_config.txt
```

Windows
```
C:\IBM\APM\samples\jboss_silent_config.txt
```

b) En el archivo `jboss_silent_config.txt`, especifique valores para todos los parámetros obligatorios. También puede modificar los valores predeterminados de otros parámetros.

Consulte la sección "Parámetros de configuración para el Agente de JBoss" en la página 485 para obtener una descripción de cada uno de los parámetros de configuración.

c) Guarde y cierre el archivo `jboss_silent_config.txt` y ejecute el mandato siguiente:

– Linux AIX *dir_instalación*`/bin/jboss-agent.sh config` **nombre_instancia** *dir_instalación*`/samples/jboss_silent_config.txt`

– Windows *dir_instalación*`\bin\jboss-agent.bat config` **nombre_instancia** *dir_instalación*`\samples\jboss_silent_config.txt`

Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

Las vías de acceso de *dir_instalación* predeterminadas se listan aquí:

– Linux `/opt/ibm/apm/agent`

– Windows `C:\IBM\APM\TMAITM6_x64`

Importante: asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

Ejemplo

Linux AIX
```
/opt/ibm/apm/agent/bin/jboss-agent.sh config example-inst01
/opt/ibm/apm/agent/samples/jboss_silent_config.txt
```

Windows
```
C:\IBM\APM\bin\jboss-agent.bat config example-inst01 C:\IBM\APM\samples
\jboss_silent_config.txt
```

d) Ejecute el mandato siguiente para iniciar el agente:

– Linux AIX *dir_instalación*`/bin/jboss-agent.sh start` **nombre_instancia**

– Windows *dir_instalación*`\bin\jboss-agent.bat start` **nombre_instancia**

Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

Las vías de acceso de *dir_instalación* predeterminadas se listan aquí:

– Linux `/opt/ibm/apm/agent`

– Windows `C:\IBM\APM\TMAITM6_x64`

Ejemplo

Linux AIX
```
/opt/ibm/apm/agent/bin/jboss-agent.sh start example-inst01
```

Windows `C:\IBM\APM\bin\jboss-agent.bat start example-inst01`

Parámetros de configuración para el Agente de JBoss

Los parámetros de configuración del Agente de JBoss se visualizan en una tabla.

1. Valores del agente de JBoss - Valores de entorno del agente de JBoss.
2. Tabla 168 en la página 486 - URLs de servicio JMX de ejemplo.

Tabla 167. Valores del agente de JBoss

Nombre de parámetro	Descripción	Nombre de parámetro del archivo de configuración silenciosa
Nombre de servidor	Proporcione un nombre para identificar el servidor JBoss/WildFly.	**KJE_SERVER**
Directorio inicial de Java	La vía de acceso en la que está instalado Java.	**JAVA_HOME**
ID de usuario de JMX	El ID de usuario para conectarse al servidor MBean.	**KQZ_JMX_JSR160_JSR160_USER_ID**
Contraseña de JMX	Contraseña	**KQZ_JMX_JSR160_JSR160_PASSWORD**
URL de servicio JMX	El URL de servicio para conectarse al servidor MBean. Consulte Tabla 168 en la página 486 para ver ejemplos.	**KQZ_JMX_JSR160_JSR160_SERVICE_URL**
Vía de acceso de clase JMX	Los archivos JAR en los que se busca para localizar una clase o recurso. Localice y especifique la vía de acceso al archivo `jboss-client.jar` del servidor JBoss. Ejemplo para un servidor JBoss EAP 6, `/opt/EAP-6.3.0/jboss-eap-6.3/bin/client/jboss-client.jar`.	**KQZ_JMX_JSR160_JSR160_JAR_FILES**
Directorio de tiempo de ejecución de DC	**Nota:** este parámetro sólo es para el Agente de JBoss con la prestación de rastreo de transacciones que se encuentra en la oferta Cloud APM, Advanced. En el caso del Agente de JBoss con capacidad de supervisión de recursos básica que se encuentra en la oferta Cloud APM, Base, omita este parámetro. La vía de acceso completa del directorio de tiempo de ejecución del recopilador de datos de JBoss se establece mediante el script **simpleConfig**. Deje este parámetro en blanco durante la configuración inicial del agente.	**KQZ_DC_RUNTIME_DIR**

Tabla 168. URLs de servicio JMX	
Versión del servidor JBoss	**URL de servicio JMX con puerto predeterminado[1]**
WildFly 8, 9 y 10 JBoss EAP 7	`service:jmx:remote+http://ip:9990` `service:jmx:remote+https://ip:9994`
JBoss EAP 6 JBoss AS 7	`service:jmx:remoting-jmx://ip:9999`
JBoss EAP 5.2 JBoss AS 6.1	`service:jmx:rmi:///jndi/rmi://ip:1090/jmxrmi`

[1] El puerto está basado en el puerto de la entrada del archivo de configuración de JBoss `<socket-binding name="management-native" interface="management" port="${jboss.management.native.port:NNNN}"/>`. Si se ha cambiado el puerto y ya no es el valor predeterminado, ajústelo según el número de puerto del archivo de configuración.

Configurar el recopilador de datos de rastreo de transacciones del Agente de JBoss

La prestación de rastreo de transacciones del Agente de JBoss requiere cambios en el archivo de valores de entorno de instancia de agente, el archivo de inicio del servidor JBoss y el parámetro de configuración de agente Directorio de tiempo de ejecución de DC. Se proporciona un script para ayudarle a hacer los cambios.

Antes de empezar

Linux Asegúrese de que el límite de recursos para archivos abiertos es mayor que 5.000 para que el kit de herramientas de rastreo de transacciones funcione adecuadamente.

- Muestra el valor límite de archivos abiertos actual. **`ulimit -n`**
- Ejemplo que establece el límite de archivos abiertos en 5.056. **`ulimit -n 5056`**

Realice el paso de Configuración del agente JBoss "1" en la página 475 o "2" en la página 476 antes de seguir este procedimiento.

El Agente de JBoss debe estar instalado localmente en el servidor JBoss supervisado con la prestación de rastreo de transacciones.

La cuenta de usuario que ejecuta este script debe tener permiso de escritura sobre los directorios y archivos siguientes:

1. El directorio *JBOSS_HOME*.
2. El directorio y los archivos de *JBOSS_HOME*`/bin`.
3. El archivo *JBOSS_HOME*`/modules/system/layers/base/org/jboss/as/server/main/module.xml`.
4. El directorio *dir_instalación*`/config`.
5. El archivo *dir_instalación*`/config/`*nombre_host*`_je_`*nombre_instancia*`.cfg`.

donde

JBOSS_HOME
Directorio de instalación del servidor JBoss.

dir_instalación
Vía de acceso donde está instalado el agente. La vía de acceso predeterminada es:

- Linux `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

nombre_host
El nombre del sistema host en el que se instala el agente.

nombre_instancia
Nombre de la instancia de agente asignada en el tema de método de configuración de agente:

- Configuración del agente en sistemas Windows, paso "3" en la página 480
- Configuración del agente respondiendo a solicitudes, paso "1" en la página 483
- Configuración del agente mediante el archivo de respuestas silencioso, paso "3" en la página 484

Procedimiento

Ejecute el script **simpleConfig**.

1. Inicie la sesión en el servidor JBoss con el Agente de JBoss instalado.
2. Vaya al directorio de instalación del agente.
   - Linux *dir_instalación*
   - Windows *dir_instalación*\TMAITM6_x64

   Donde *dir_instalación* es la vía de acceso donde está instalado el agente.

   Las vías de acceso de *dir_instalación* predeterminadas se listan aquí:
   - Linux /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64
3. Vaya al directorio jedchome/7.3.0.13.0/bin.
4. Ejecute el script de configuración.
   - Linux ./simpleConfig.sh
   - Windows simpleConfig.bat
5. Siga las indicaciones para especificar parámetros para su entorno:
   a) Especifique el *nombre_instancia* de Agente de JBoss elegido para la instancia de agente.
   b) Especifique el directorio de instalación del servidor JBoss.
      Si la variable de entorno *JBOSS_HOME* está establecida, el valor correspondiente se ofrecerá como el valor predeterminado.

   donde

   JBOSS_HOME
   Directorio de instalación de JBoss Server.

   nombre_instancia
   El nombre de la instancia de agente asignada en el tema de método de configuración de agente:
   - Configuración del agente en sistemas Windows, paso "3" en la página 480
   - Configuración del agente respondiendo a solicitudes, paso "1" en la página 483
   - Configuración del agente mediante el archivo de respuestas silencioso, paso "3" en la página 484

   dir_instalación
   La vía de acceso donde está instalado el agente. La vía de acceso predeterminada es:
   - Linux /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64
6. Reinicie el servidor JBoss y el agente si se están ejecutando.

Resultados

Archivos de servidor JBoss cambiados durante la configuración del rastreo de transacciones:

- *JBOSS_HOME*/bin/standalone.conf

  Este archivo se actualiza con valores de configuración necesarios para la prestación de rastreo de transacciones. Los marcadores de configuración se insertan en el archivo para utilizarlos al inhabilitar la prestación de rastreo de transacciones. Se guarda un archivo de copia de seguridad en el directorio *JBOSS_HOME*/bak antes de añadir o eliminar los cambios en la prestación de rastreo de transacciones.
- *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml

  Este archivo se actualiza con una dependencia de módulo de API de JAVA EE. Los marcadores de configuración se insertan en el archivo para utilizarlos al inhabilitar la prestación de rastreo de transacciones. Se guarda un archivo de copia de seguridad en el directorio *JBOSS_HOME*/bak antes de añadir o eliminar los cambios en la prestación de rastreo de transacciones.

Archivos de agente cambiados durante la configuración del rastreo de transacciones:

- Archivo de configuración de instancia de agente
  - Linux *dir_instalación*/config/*nombre_host*_je_*nombre_instancia*.cfg
  - Windows *dir_instalación*\TMAITM6_x64*nombre_host*_JE_*nombre_instancia*.cfg
- Archivo de valores de entorno de agente
  - Linux *dir_instalación*/config/je_*nombre_instancia*.environment
  - Windows *dir_instalación*\TMAITM6_x64\KJEENV_*nombre_instancia*

donde

JBOSS_HOME
Directorio de instalación del servidor JBoss.

dir_instalación
Vía de acceso donde está instalado el agente. La vía de acceso predeterminada es:

- Linux /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

nombre_host
El nombre del sistema host en el que se instala el agente.

nombre_instancia
Nombre de la instancia de agente asignada en el tema de método de configuración de agente:

- Configuración del agente en sistemas Windows, paso "3" en la página 480
- Configuración del agente respondiendo a solicitudes, paso "1" en la página 483
- Configuración del agente mediante el archivo de respuestas silencioso, paso "3" en la página 484

Inhabilitar el recopilador de datos de rastreo de transacciones del Agente de JBoss
La prestación de rastreo de transacciones del Agente de JBoss requiere cambios en el archivo de valores de entorno de instancia de agente, el archivo de inicio del servidor JBoss y el parámetro de configuración de agente Directorio de tiempo de ejecución de DC. Se proporciona un script para eliminar estos cambios para una instancia de agente con el rastreo de transacciones habilitado.

Antes de empezar

Asegúrese de haber concluido el servidor JBoss y el Agente de JBoss.

La cuenta de usuario que ejecuta este script debe tener permiso de escritura sobre los directorios y archivos siguientes:

1. El directorio *JBOSS_HOME*
2. El directorio *JBOSS_HOME*/bin y los archivos
3. El archivo *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml

4. El directorio *dir_instalación*/config
5. El archivo *dir_instalación*/config/*nombre_host*_je_*nombre_instancia*.cfg

Procedimiento

Ejecute el script **simpleConfig** con la opción **remove**.

1. Inicie la sesión en el servidor JBoss con el Agente de JBoss instalado.
2. Vaya al directorio de instalación del agente.
   - Linux *dir_instalación*
   - Windows *dir_instalación*\TMAITM6_x64
3. Vaya al directorio jedchome/7.3.0.13.0/bin.
4. Ejecute **simpleConfig** con la opción **remove**.
   - Linux ./simpleConfig.sh **remove** *nombre_instancia*
   - Windows simpleConfig.bat **remove** *nombre_instancia*
5. Inicie el servidor JBoss y el agente.

   Donde:

   JBOSS_HOME
   Directorio de instalación de JBoss Server.

   nombre_host
   Nombre del sistema host en el que se instala el agente.

   nombre_instancia
   Nombre de la instancia de agente asignada en el tema de método de configuración de agente:
   - Configuración del agente en sistemas Windows, paso "3" en la página 480
   - Configuración del agente respondiendo a solicitudes, paso "1" en la página 483
   - Configuración del agente mediante el archivo de respuestas silencioso, paso "3" en la página 484

   dir_instalación
   Vía de acceso donde está instalado el agente. La vía de acceso predeterminada es:
   - Linux /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64

   arquitectura
   Identificador de la arquitectura del sistema IBM Application Performance Management o Cloud APM. Por ejemplo, lx8266 representa Linux Intel v2.6 (64 bits). Para obtener una lista completa de los códigos de arquitectura, consulte el archivo *dir_instalación*/registry/archdsc.tbl.

Desinstalar todo el rastreo de transacciones de Agente de JBoss

La prestación de rastreo de transacciones de Agente de JBoss se puede desinstalar. Se proporciona un script para eliminar todas las instancias de agente con rastreo de transacciones habilitado y para eliminar también el kit de herramientas de rastreo de transacciones.

Antes de empezar

Asegúrese de que haber concluido el servidor JBoss y todas las instancias del Agente de JBoss.

La cuenta de usuario que ejecuta este script debe tener permiso de escritura sobre los directorios y archivos siguientes:

1. El directorio *JBOSS_HOME*.
2. El directorio y los archivos de *JBOSS_HOME*/bin.

3. El archivo *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml.
4. El directorio *dir_instalación*/config.
5. El archivo *dir_instalación*/config/*nombre_host*_je_*nombre_instancia*.cfg.

Procedimiento

Ejecute el script **simpleConfig** con la opción **uninstall**.

1. Inicie la sesión en el servidor JBoss con el Agente de JBoss instalado.
2. Vaya al directorio de instalación del agente.
   - Linux *dir_instalación*/*arquitectura*/je/bin. Por ejemplo: /opt/ibm/apm/agent/lx8266/je/bin o /opt/ibm/apm/agent/lx8266/je/bin
   - Windows *dir_instalación*\TMAITM6_x64
3. Vaya al directorio jedchome/7.3.0.13.0/bin.
4. Ejecute **simpleConfig** con la opción **uninstall**.
   - Linux ./simpleConfig.sh **uninstall**
   - Windows simpleConfig.bat **uninstall**
5. Inicie el servidor JBoss y todas las instancias de agente.

Donde:

JBOSS_HOME
Directorio de instalación de JBoss Server.

nombre_host
El nombre del sistema host en el que se instala el agente.

nombre_instancia
El nombre de la instancia de agente asignada en el tema de método de configuración de agente:

- Configuración del agente en sistemas Windows, paso "3" en la página 480
- Configuración del agente respondiendo a solicitudes, paso "1" en la página 483
- Configuración del agente mediante el archivo de respuestas silencioso, paso "3" en la página 484

dir_instalación
La vía de acceso donde está instalado el agente. La vía de acceso predeterminada es:

- Linux /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

arquitectura
Identificador de la arquitectura del sistema IBM Application Performance Management o Cloud APM. Por ejemplo, lx8266 representa Linux Intel v2.6 (64 bits). Para obtener una lista completa de los códigos de arquitectura, consulte el archivo *dir_instalación*/registry/archdsc.tbl.

Configuración de la supervisión de Linux KVM

Debe configurar el Monitoring Agent for Linux KVM para recopilar datos de los servidores Red Hat Enterprise Virtualization Hypervisor (RHEVH) y Red Hat Enterprise Virtualization Manager (RHEVM). Después de instalar el agente en un servidor una máquina virtual, debe crear la primera instancia e iniciar manualmente el agente.

Antes de empezar
Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Linux KVM.

Acerca de esta tarea
El Agente de Linux KVM es un agente de varias instancias y varias conexiones. Varias instancias significa que puede crear varias instancias y cada instancia puede realizar varias conexiones a uno o más servidores RHEVM o RHEVH.

Recuerde: utilice instancias diferentes para supervisar los servidores RHEVM o RHEVH.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte “Historial de cambios” en la página 52.

Puede utilizar el mismo script de configuración para configurar instancias para los servidores RHEVM y RHEVH:

- Para configurar una conexión con el servidor RHEVM, siga los pasos indicados en el tema "Configuración de una conexión con el servidor RHEVM".
- Para configurar una conexión con el servidor RHEVH, siga los pasos indicados en el tema "Configuración de una conexión con el servidor RHEVH".

Cómo crear un usuario y otorgar los permisos necesarios

Antes de configurar el Agente de Linux KVM, debe crear un usuario y otorgarle los permisos necesarios para supervisar los servidores RHEVM y RHEVH.

Procedimiento

1. Abra el portal **Red Hat Enterprise Virtualization Manager Web Administration** .
2. Pulse **Configure**.
3. En la ventana **Configuration**, seleccione **Roles**.
   a) Para crear un rol, pulse **New**.
   b) En la ventana **New Role**, añada el nombre del rol y seleccione **Admin** como el tipo de cuenta.
   c) Asegúrese de que los recuadros de selección del panel **Check boxes to Allow Action** no están seleccionados y pulse **OK**.
4. En la ventana **Configuration**, seleccione **System Permission**.
   a) Para otorgar un permiso de usuario, pulse **Add**.
   b) En la ventana **Add System Permission to User**, seleccione el usuario a quien desea otorgar el permiso.
   c) En la lista **Assign role to user**, seleccione el rol que ha creado y pulse **OK**.

Qué hacer a continuación
Complete la configuración del agente:

- “Configuración de una conexión con el servidor RHEVH” en la página 497
- “Configuración de una conexión con el servidor RHEVM” en la página 496

Configuración de protocolos

El agente utiliza protocolos distintos para conectarse al servidor RHEVH. Puede configurar cualquiera de estos protocolos: SSH, TLS o TCP.

Acerca de esta tarea
El Agente de Linux KVM se conecta de forma remota a cada hipervisor utilizando la herramienta **virsh** que gestiona las máquinas virtuales QEMU-KVM y recopila métricas. La API `libvirt` del entorno de agente utiliza varios protocolos de transporte remoto diferentes. Para obtener la lista de protocolos soportados, consulte la página de soporte remoto.

Configuración del protocolo SSH
Puede configurar el protocolo SSH para supervisar un host de forma remota.

Acerca de esta tarea
Asunción: el Agente de Linux KVM está instalado en el host A. Desea supervisar remotamente el hipervisor en el host B.

Procedimiento

1. Inicie la sesión en el host A con el mismo ID de usuario que ejecuta el proceso del Agente de Linux KVM, por ejemplo, el ID de usuario root.

   Consejo: asegúrese de que conoce el ID en el host B que acepta la conexión SSH y el ID de usuario root en el host A.
2. Genere las claves **id_rsa** y **id_rsa.pub** en el host A mediante el programa de utilidad *ssh-keygen*.
   Las claves se guardan en la ubicación siguiente: `~/.ssh: $ ssh-keygen -t rsa`.
3. Copie las claves autorizadas del host B:

   $ scp Id del host B@name o dirección IP de host B:~/.ssh/claves_autorizadas ~/.ssh/claves_autorizadas_de_B
4. Añada la clave pública para el host A al final de las claves autorizadas para el host B:

   cat ~/.ssh/id_rsa.pub >> ~/.ssh/claves_autorizadas_de_B
5. Copie de nuevo las claves autorizadas en el host B:

   $ scp ~/.ssh/claves_autorizadas_de_B Id de B@name o dirección IP de host B:~/.ssh/claves_autorizadas

   Recuerde: si está supervisando varios hosts, repita los pasos "3" en la página 492, "4" en la página 492 y "5" en la página 492 para cada host.
6. Elimine las claves autorizadas que ha copiado en el host B:

   ~/.ssh/claves_autorizadas_de_B
7. Añada el mandato siguiente al perfil **~/.bash_** del ID actual en el host A:

   $ eval `ssh-agent`

   Recuerde: Asegúrese de que utiliza la comilla simple invertida (`), que se encuentra debajo de la tilde (~) en teclados de EE.UU., y no la comilla simple (').
8. Añada la identidad al host A y especifique la contraseña que ha utilizado al crear el ID:

   $ ssh-add ~/.ssh/id_rsa
9. Ejecute el mandato siguiente si recibe el mensaje `No se ha podido abrir una conexión al agente de autenticación`:

   exec ssh-agent bash

   Consejo: Puede sustituir la bash por la shell que está utilizando y a continuación ejecutar de nuevo el mandato siguiente:

   $ ssh-add ~/.ssh/id_rsa
10. Pruebe el protocolo SSH para asegurarse de que se conecta desde el host A al host B sin necesidad de especificar la contraseña SSH:

    Consejo: si está supervisando varios hosts, utilice el mandato siguiente para probar la conexión para cada host:

```
$ ssh Id en host B@name o dirección IP de host B
```

11. Para verificar la conexión, ejecute el mandato siguiente:

    ```
    virsh -c qemu+ssh://Id on host B@name or IP address of host B:port/system
    ```

    Si no ha cambiado el puerto SSH predeterminado, omita la sección **:port** del mandato.

    Importante: si el mandato **virsh** es satisfactorio, el Agente de Linux KVM se conectará al hipervisor.
12. Debe reiniciar el host A antes de reiniciar el Agente de Linux KVM en el host A. Para reiniciar, debe volver a ejecutar el mandato **ssh-add** y especificar la contraseña cada vez.

    Consejo: puede utilizar cadenas de clave SSH para evitar volver a especificar la contraseña.

Configuración del protocolo TLS

Puede configurar el protocolo TLS para supervisar un host de forma remota.

Acerca de esta tarea

Asunción: el Agente de Linux KVM está instalado en el host A. Desea supervisar remotamente el hipervisor en el host B.

Procedimiento

1. Para crear una clave de una entidad emisora de certificados (CA) y un certificado en el hipervisor, siga estos pasos:
   a) Inicie la sesión en host B.
   b) Cree un directorio temporal y cambie la vía de acceso a este directorio temporal:

   ```
   mkdir cert_files
   cd cert_files
   ```

   c) Cree una clave RSA de 2048 bits:

   ```
   openssl genrsa -out cakey.pem 2048
   ```

   d) Cree un certificado firmado automáticamente para la CA local:

   ```
   openssl req -new -x509 -days 1095 -key cakey.pem -out \
   cacert.pem -sha256 -subj "/C=US/L=Austin/O=IBM/CN=my CA"
   ```

   e) Compruebe el certificado de la CA:

   ```
   openssl x509 -noout -text -in cacert.pem
   ```

2. Para crear las claves y certificados de cliente y servidor en el hipervisor, siga estos pasos:
   a) Cree las claves:

   ```
   openssl genrsa -out serverkey.pem 2048
   openssl genrsa -out clientkey.pem 2048
   ```

   b) Cree una solicitud de firma de certificado para el servidor:

   Recuerde: cambie la dirección kvmhost.company.org, que se utiliza en la solicitud de certificado de servidor, por el nombre de dominio completo del host del hipervisor.

   ```
   openssl req -new -key serverkey.pem -out serverkey.csr \
   -subj "/C=US/O=IBM/CN=kvmhost.company.org"
   ```

   c) Cree una solicitud de firma de certificado para el cliente:

   ```
   openssl req -new -key clientkey.pem -out clientkey.csr \
   -subj "/C=US/O=IBM/OU=virtualization/CN=root"
   ```

   d) Cree los certificados de cliente y servidor:

   ```
   openssl x509 -req -days 365 -in clientkey.csr -CA cacert.pem \
   -CAkey cakey.pem -set_serial 1 -out clientcert.pem
   ```

```
openssl x509 -req -days 365 -in serverkey.csr -CA cacert.pem \
-CAkey cakey.pem -set_serial 94345 -out servercert.pem
```

e) Compruebe las claves:

```
openssl rsa -noout -text -in clientkey.pem
```

```
openssl rsa -noout -text -in serverkey.pem
```

f) Compruebe los certificados:

```
openssl x509 -noout -text -in clientcert.pem
```

```
openssl x509 -noout -text -in servercert.pem
```

3. Para distribuir las claves y certificados al servidor de host, siga estos pasos:

a) Copie el archivo `cacert.pem` del certificado de CA en este directorio: `/etc/pki/CA`

```
cp cacert.pem /etc/pki/CA/cacert.pem
```

b) Cree el directorio `/etc/pki/libvirt` y copie el archivo de certificado del servidor `servercert.pem` en el directorio `/etc/pki/libvirt`. Asegúrese de que sólo el usuario root pueda acceder a la clave privada.

```
mkdir /etc/pki/libvirt
```

```
cp servercert.pem /etc/pki/libvirt/.
```

```
chmod -R o-rwx /etc/pki/libvirt
```

Recuerde: si las claves o certificados se denominan incorrectamente o se copian en los directorios incorrectos, la autorización fallará.

c) Cree el directorio `/etc/pki/libvirt/private` y copie el archivo de claves del servidor `serverkey.pem` en el directorio `/etc/pki/libvirt/private`. Asegúrese de que sólo el usuario root pueda acceder a la clave privada.

```
mkdir /etc/pki/libvirt/private
```

```
cp serverkey.pem /etc/pki/libvirt/private/.
```

```
chmod -R o-rwx /etc/pki/libvirt/private
```

Recuerde: si las claves o certificados se denominan incorrectamente o se copian en los directorios incorrectos, la autorización fallará.

d) Verifique que los archivos se han colocado correctamente:

```
find /etc/pki/CA/*|xargs ls -l
```

```
ls -lR /etc/pki/libvirt
```

```
ls -lR /etc/pki/libvirt/private
```

Recuerde: si las claves o certificados se denominan incorrectamente o se copian en los directorios incorrectos, la autorización fallará.

4. Para distribuir las claves y certificados a los clientes o estaciones de gestión, siga estos pasos:

a) Inicie la sesión en host A.

b) Copie el archivo `cacert.pem` del certificado de CA del host en el directorio `/etc/pki/CA` del host A sin cambiar el nombre de archivo.

```
scp kvmhost.company.org:/tmp/cacert.pem /etc/pki/CA/
```

c) Copie el archivo `clientcert.pem` del certificado de cliente en el directorio `/etc/pki/libvirt` del host B. Utilice el nombre de archivo predeterminado y asegúrese de que sólo el usuario root pueda acceder a la clave privada.

```
mkdir /etc/pki/libvirt/
```

```
scp kvmhost.company.org:/tmp/clientcert.pem /etc/pki/libvirt/.
```

```
chmod -R o-rwx /etc/pki/libvirt
```

Recuerde: si las claves o certificados se denominan incorrectamente o se copian en los directorios incorrectos, la autorización fallará.

d) Copie la clave de cliente `clientkey.pem` en el directorio `/etc/pki/libvirt/private` del host. Utilice los nombres de archivo predeterminados y asegúrese de que sólo el usuario root pueda acceder a la clave privada.

mkdir /etc/pki/libvirt/private

scp kvmhost.company.org:/tmp/clientkey.pem /etc/pki/libvirt/private/.

chmod -R o-rwx /etc/pki/libvirt/private

Recuerde: si las claves o certificados se denominan incorrectamente o se copian en los directorios incorrectos, la autorización fallará.

e) Verifique que los archivos se han colocado correctamente:

ls -lR /etc/pki/libvirt

ls -lR /etc/pki/libvirt/private

5. Para editar la configuración del daemon `libvirtd`, realice los pasos siguientes:
   a) Inicie la sesión en host B.
   b) Haga una copia del archivo `/etc/sysconfig/libvirtd` y del archivo `/etc/libvirt/libvirtd.conf`.
   c) Edite el archivo `/etc/sysconfig/libvirtd` y asegúrese de que el parámetro **--listen** se pasa al daemon `libvirtd`. Este paso garantiza que el daemon `libvirtd` está a la escucha de conexiones de red.
   d) Edite el archivo `/etc/libvirt/libvirtd.conf` y configure un conjunto de sujetos permitidos con la directiva **tls_allowed_dn_list** en el archivo `libvirtd.conf`.

      Importante: los campos del sujeto deben estar en el mismo orden que ha utilizado para crear el certificado.

   e) Reinicie el servicio de daemon `libvirtd` para que los cambios entren en vigor:

      /etc/init.d/libvirtd restart
6. Para cambiar la configuración del cortafuegos, acceda a la configuración de nivel de seguridad y añada el puerto TCP 16514 como puerto de confianza.
7. Para verificar que la gestión remota está funcionando, ejecute el mandato siguiente en el host A:

   virsh -c qemu+tls://kvmhost.company.org/system list --all

Configuración del protocolo TCP
Utilice el protocolo TCP sólo para realizar pruebas.

Acerca de esta tarea
Asunción: el Agente de Linux KVM está instalado en el host A. Desea supervisar remotamente el hipervisor en el host B.

Procedimiento

1. Inicie la sesión en host B.
2. Edite el archivo `/etc/libvirt/libvirtd.conf` y asegúrese de que el parámetro **listen_tcp** está habilitado y de que el valor del parámetro **tcp_port** está establecido en el valor predeterminado 16509.
3. Edite el archivo `/etc/libvirt/libvirtd.conf` para establecer el parámetro **auth_tcp** en "none". Este paso indica a TCP que no debe autenticar la conexión.
4. Reinicie el daemon **libvirt** en el host B en modalidad de escucha ejecutándolo con el indicador **--listen** o editando el archivo `/etc/sysconfig/libvirtd` y eliminando el comentario de la línea `LIBVIRTD_ARGS="--listen"`.

5. Para verificar la conexión, ejecute el mandato siguiente:

   virsh -c qemu+tcp://kvmhost.company.org:port/system

   Si no ha cambiado el puerto TCP predeterminado, omita la sección **:port** del mandato.

   Importante: si el mandato **virsh** es satisfactorio, el Agente de Linux KVM se conectará al hipervisor.

Qué hacer a continuación
Configure el agente siguiendo los pasos descritos en la sección "Configuración de una conexión con el servidor RHEVH" en la página 497.

Configuración de una conexión con el servidor RHEVM

Para configurar una conexión con el servidor RHEVM, debe ejecutar el script y responder a las solicitudes.

Antes de empezar

1. Descargue el certificado de seguridad que está disponible en la siguiente vía de acceso:

   ```
   https://HOST-RHEVM:PUERTO-RHEVM/ca.crt
   ```

   Donde

   HOST-RHEVM
   El nombre del host.

   PUERTO-RHEVM
   El puerto utilizado en el entorno RHEVM.

2. Utilice el programa de utilidad *keytool* para importar el archivo de certificado de seguridad para generar un archivo de almacén de claves local:

   keytool -import -alias ALIAS -file ARCHIVO_CERTIFICADO -keystore ARCHIVO_ALMACÉN_CLAVES

   Ejemplo: **keytool -import -alias RHEVM36vmwt9 -file hjs495-vmw-t-9.cer -keystore RHEVM36KeyStore**

   Donde

   ALIAS
   Una referencia exclusiva para cada certificado que se añade al almacén de confianza del agente; por ejemplo, un alias adecuado para el certificado de *origendatos.ejemplo.com* sería *origendatos*.

   ARCHIVO_CERTIFICADO
   La vía de acceso completa y el nombre de archivo para el certificado de origen de datos que se añade al almacén de confianza.

   ARCHIVO_ALMACÉN_CLAVES
   El nombre del archivo de almacén de claves que desea especificar.

   Consejo: el programa de utilidad *keytool* está disponible con Java Runtime Environment (JRE). El archivo de almacén de claves se almacena en la misma ubicación desde la que se ejecuta el mandato.

3. Asegúrese de que el usuario que se conecta a RHEVM sea un administrador con el rol SuperUser. Puede utilizar un ID de usuario existente con este rol o crear un ID de usuario siguiendo los pasos indicados en la sección "Cómo crear un usuario y otorgar los permisos necesarios" en la página 491.

Procedimiento

1. En la línea de mandatos, ejecute el mandato siguiente:

   dir_instalación/bin/linux_kvm-agent.sh config nombre_instancia

   Ejemplo: **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh config nombre_instancia**

   Donde

nombre_instancia
El nombre que desea dar a la instancia.

dir_instalación
La vía de acceso donde está instalado el agente.

2. Responda a las solicitudes y especifique valores para los parámetros de configuración.

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración para conectarse al servidor RHEVM" en la página 498.

3. Ejecute el mandato siguiente para iniciar el agente:

   dir_instalación/bin/linux_kvm-agent.sh start nombre_instancia

   Ejemplo: **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh start nombre_instancia**

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración de una conexión con el servidor RHEVH

Para configurar una conexión con el servidor RHEVH, debe ejecutar el script y responder a las solicitudes.

Antes de empezar

- Asegúrese de que el usuario que se conecta a RHEVM es un usuario root. Puede utilizar un ID de usuario existente o crear un ID de usuario siguiendo los pasos indicados en la sección "Cómo crear un usuario y otorgar los permisos necesarios" en la página 491.
- Configure el protocolo que desee utilizar para conectarse al servidor RHEVH siguiendo los pasos descritos en la sección "Configuración de protocolos" en la página 491.

Procedimiento

1. En la línea de mandatos, ejecute el mandato siguiente:

   dir_instalación/bin/linux_kvm-agent.sh config nombre_instancia

   Ejemplo: **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh config nombre_instancia**

   Donde

   nombre_instancia
   El nombre que desea dar a la instancia.

   dir_instalación
   La vía de acceso donde está instalado el agente.

2. Responda a las solicitudes y especifique valores para los parámetros de configuración.

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración para conectarse al servidor RHEVH" en la página 500.

3. Ejecute el mandato siguiente para iniciar el agente:

   dir_instalación/bin/linux_kvm-agent.sh start nombre_instancia

   Ejemplo: **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh start nombre_instancia**

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Parámetros de configuración para conectarse al servidor RHEVM

Puede modificar los valores predeterminados de los parámetros de configuración que se utilizan para conectar el agente con el servidor RHEVM.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración.

Tabla 169. Nombres y descripciones de los parámetros de configuración para conectarse al servidor RHEVM

Nombre de parámetro	**Descripción**	**Campo obligatorio**
Editar valores de Monitoring Agent for Linux KVM	Indica que puede empezar a editar los valores predeterminados de los parámetros de configuración. Especifique `1 (Sí)`, que es también el valor predeterminado, para continuar.	Sí
Número máximo de archivos de registro del proveedor de datos	El número máximo de archivos de registro que el proveedor de datos crea antes de grabar encima de los archivos de registro anteriores. El valor predeterminado es 10.	Sí
Tamaño máximo en KB de cada archivo de registro del proveedor de datos	El tamaño máximo en KB que debe alcanzar un archivo de registro del proveedor de datos antes de que el proveedor de datos cree un archivo de registro nuevo. El valor predeterminado es 5190 KB.	Sí

Tabla 169. Nombres y descripciones de los parámetros de configuración para conectarse al servidor RHEVM (continuación)

Nombre de parámetro	Descripción	Campo obligatorio
Nivel de detalle en el archivo de registro del proveedor de datos	El nivel de detalle que puede incluirse en el archivo de registro que crea el proveedor de datos. El valor predeterminado es 4 (Info). Los valores siguientes son válidos: • 1= Desactivado: no se registra ningún mensaje. • 2 = Grave: sólo se registran los errores. • 3 = Aviso: todos los errores y mensajes que se registran en el nivel Grave y los errores potenciales que pueden provocar un comportamiento indeseable. • 4 = Info: todos los errores y mensajes que se registran en el nivel Aviso y los mensajes informativos de alto nivel que describen el estado del proveedor de datos cuando se procesa. • 5 = Bueno: todos los errores y mensajes que se registran en el nivel Info y los mensajes informativos de bajo nivel que describen el estado del proveedor de datos cuando se procesa. • 6 = Mejor: todos los errores y mensajes que se registran en el nivel Bueno y los mensajes informativos muy detallados, como por ejemplo la información de perfilado de rendimiento y datos de depuración. Si selecciona esta opción, el rendimiento del agente de supervisión puede verse perjudicado. Este valor está concebido para utilizarlo como herramienta para la determinación de problemas en colaboración con el personal de soporte de IBM. • 7 = El mejor: todos los errores y mensajes que se registran en el nivel Bueno y los mensajes informativos más detallados que incluyen datos y mensajes de programación de bajo nivel. Si selecciona esta opción, el rendimiento del agente de supervisión puede verse perjudicado. Este valor está concebido para utilizarlo como herramienta para la determinación de problemas en colaboración con el personal de soporte de IBM. • 8 = Todos: se registran todos los mensajes.	Sí
Editar valores de hipervisor	Indica si se desean editar los parámetros para una conexión al servidor RHEVH. Especifique `5 (Añadir)`, ya que está configurando una conexión al servidor RHEVM. El valor predeterminado es `5 (Siguiente)`.	Sí
Editar valores de detalles de conexión RHEVM	Indica si se desean editar los parámetros para una conexión al servidor RHEVM. Especifique `1 (Añadir)` para continuar. El valor predeterminado es `5 (Siguiente)`. **Importante:** después de especificar valores para todos los parámetro de configuración, se le solicitará de nuevo que indique si desea continuar editando los parámetros. Especifique `5 (Salir)`.	Sí
ID de RHEVM	El nombre de usuario exclusivo, que se especifica para el RHEVM al que se conecta.	Sí
Host	El nombre de host o dirección IP del origen de datos que se utiliza para conectarse al servidor RHEVM.	Sí

Tabla 169. Nombres y descripciones de los parámetros de configuración para conectarse al servidor RHEVM (continuación)		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Usuario	El nombre de usuario del origen de datos con privilegios suficientes para conectarse al servidor RHEVM.	Sí
Contraseña	La contraseña del nombre de usuario utilizado para conectarse al servidor RHEVM.	Sí
Volver a escribir la contraseña	La misma contraseña que ha especificado en el campo **Contraseña**.	Sí
Puerto	El número de puerto utilizado para conectarse al servidor RHEVM.	Sí
Dominio	El dominio al que pertenece el usuario.	Sí
KeyStorePath	El nombre y vía de acceso del archivo de almacén de claves local que ha creado mediante el mandato **keytool**.	Sí

Parámetros de configuración para conectarse al servidor RHEVH

Puede modificar los valores predeterminados de los parámetros de configuración que se utilizan para conectar el agente con el servidor RHEVH.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración.

Tabla 170. Nombres y descripciones de los parámetros de configuración para conectarse al hipervisor		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Editar valores de Monitoring Agent for Linux KVM	Indica que puede empezar a editar los valores predeterminados de los parámetros de configuración. Especifique `1 (Sí)`, que es también el valor predeterminado, para continuar.	Sí
Número máximo de archivos de registro del proveedor de datos	El número máximo de archivos de registro que el proveedor de datos crea antes de grabar encima de los archivos de registro anteriores. El valor predeterminado es 10.	Sí
Tamaño máximo en KB de cada archivo de registro del proveedor de datos	El tamaño máximo en KB que debe alcanzar un archivo de registro del proveedor de datos antes de que el proveedor de datos cree un archivo de registro nuevo. El valor predeterminado es 5190 KB.	Sí

Tabla 170. Nombres y descripciones de los parámetros de configuración para conectarse al hipervisor (continuación)

Nombre de parámetro	Descripción	Campo obligatorio
Nivel de detalle en el archivo de registro del proveedor de datos	El nivel de detalle que puede incluirse en el archivo de registro que crea el proveedor de datos. El valor predeterminado es 4 (Info). Los valores siguientes son válidos: • 1= Desactivado: no se registra ningún mensaje. • 2 = Grave: sólo se registran los errores. • 3 = Aviso: todos los errores y mensajes que se registran en el nivel Grave y los errores potenciales que pueden provocar un comportamiento indeseable. • 4 = Info: todos los errores y mensajes que se registran en el nivel Aviso y los mensajes informativos de alto nivel que describen el estado del proveedor de datos cuando se procesa. • 5 = Bueno: todos los errores y mensajes que se registran en el nivel Info y los mensajes informativos de bajo nivel que describen el estado del proveedor de datos cuando se procesa. • 6 = Mejor: todos los errores y mensajes que se registran en el nivel Bueno y los mensajes informativos muy detallados, como por ejemplo la información de perfilado de rendimiento y datos de depuración. Si selecciona esta opción, el rendimiento del agente de supervisión puede verse perjudicado. Este valor está concebido para utilizarlo como herramienta para la determinación de problemas en colaboración con el personal de soporte de IBM. • 7 = El mejor: todos los errores y mensajes que se registran en el nivel Bueno y los mensajes informativos más detallados que incluyen datos y mensajes de programación de bajo nivel. Si selecciona esta opción, el rendimiento del agente de supervisión puede verse perjudicado. Este valor está concebido para utilizarlo como herramienta para la determinación de problemas en colaboración con el personal de soporte de IBM. • 8 = Todos: se registran todos los mensajes.	Sí
Editar valores de hipervisor	Indica si se desean editar los parámetros para una conexión de hipervisor. Especifique `1 (Añadir)`. El valor predeterminado es `5 (Siguiente)`.	Sí
ID de hipervisor	El nombre de usuario exclusivo, que se especifica para el RHEVH al que se conecta.	Sí
Host	El nombre de host o dirección IP del origen de datos que se utiliza para conectarse al servidor RHEVH.	Sí
Usuario	Un nombre de usuario del origen de datos con privilegios suficientes para conectarse al servidor RHEVM.	Sí

Tabla 170. Nombres y descripciones de los parámetros de configuración para conectarse al hipervisor (continuación)

Nombre de parámetro	Descripción	Campo obligatorio
Transporte remoto	El protocolo utilizado por la API `libvirt` local para conectarse a las API `libvirt` remotas. El valor predeterminado es 1. Los valores siguientes son válidos: • 1 = SSH • 2 = TLS • 3 = TCP (Sin cifrar - no recomendado para uso en producción).	Sí
Puerto	El puerto utilizado por el protocolo de transporte para conectarse a la API `libvirt`. El valor predeterminado es 22. **Importante:** este puerto sólo es necesario si se han cambiado los puertos estándar (22 para SSH, 16514 para TLS, 16509 para TCP).	Sí
Dominio	El dominio al que pertenece el usuario.	Sí
Tipo de instancia de conexión	Indica si la API `libvirt` local se conecta al controlador del sistema con privilegios o al controlador de sesión sin privilegios en función del usuario. El valor predeterminado es 1. Los valores siguientes son válidos: • 1 = sistema • 2 = sesión	Sí
Editar valores de detalles de conexión RHEVM	Indica si se desean editar los parámetros para una conexión al servidor RHEVM. Especifique `1 (Añadir)` para continuar. El valor predeterminado es `5 (Siguiente)`. **Importante:** después de especificar valores para todos los parámetro de configuración, se le solicitará de nuevo que indique si desea continuar editando los parámetros. Especifique 5 `(Siguiente)`.	Sí

Configuración de la supervisión de MariaDB

Debe configurar el Agente de MariaDB para que el agente pueda recopilar datos para supervisar la disponibilidad y el rendimiento de los recursos del servidor MariaDB. Consulte los siguientes requisitos previos para configurar el agente de MariaDB para la supervisión remota y local.

Antes de empezar

Asegúrese de que los requisitos del sistema del Agente de MariaDB se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de MariaDB.

Acerca de esta tarea

El agente de MariaDB es un agente de instancia única. Debe configurar el agente manualmente una vez esté instalado. Puede configurar el agente en los sistemas operativos Windows y Linux. El agente requiere un nombre de instancia y las credenciales de usuario del servidor MariaDB. El nombre de sistema gestionado incluye el nombre de instancia que especifique, por ejemplo, *nombre_instancia*:*nombre_host*:*pc*, donde *pc* es el código de producto de dos caracteres. El nombre de sistema gestionado puede contener hasta 32 caracteres. El nombre de instancia que

especifique puede contener hasta 28 caracteres, excluida la longitud del nombre de host. Por ejemplo, si especifica `MariaDB` como nombre de instancia, el nombre de sistema gestionado será `MariaDB:nombrehost:MJ`.

Importante: Si especifica un nombre de instancia largo, el nombre de sistema gestionado queda truncado y el código de agente no se visualiza.

Configuración del agente en sistemas Windows

Puede configurar el agente en sistemas operativos Windows utilizando la ventana IBM Cloud Application Performance Management. Después de actualizar los valores de configuración, inicie el agente para aplicar los valores actualizados.

Procedimiento

Para configurar el agente en sistemas operativos Windows, realice los siguientes pasos:

1. Pulse **Inicio > Todos los programas > Agentes de IBM Monitoring > IBM Performance Management**.
2. En la ventana **IBM Performance Management**, complete estos pasos:
   a) Efectúe una doble pulsación en la plantilla **Monitoring Agent for MariaDB**.
   b) En la ventana **Monitoring Agent for MariaDB**, especifique un nombre de instancia y pulse **Aceptar**.
3. En la ventana **Monitoring Agent for MariaDB**, siga estos pasos:
   a) En el campo **Dirección IP**, especifique la dirección IP del servidor MariaDB que desee supervisar de forma remota. Si el agente está instalado en un servidor que se va a supervisar, retenga el valor predeterminado.
   b) En el campo **Nombre de usuario de JDBC** especifique el nombre de un usuario de servidor MariaDB. El valor predeterminado es root.
   c) En el campo **Contraseña de JDBC**, escriba la contraseña de un usuario de JDBC.
   d) En el campo **Confirmar contraseña de JBDC**, escriba de nuevo la contraseña.
   e) En el campo **Archivo .jar de JDBC**, pulse **Examinar** y localice el directorio que contiene el archivo Java del conector MariaDB y selecciónelo.
   f) Pulse **Siguiente**.
   g) En el campo **Número de puerto JDBC**, especifique el número de puerto del servidor JDBC.
   El número de puerto predeterminado es 3306.
   h) En la lista **Nivel de rastreo de Java**, seleccione un nivel de rastreo para Java.
   El valor predeterminado es `Error`.
   i) Pulse **Aceptar**.
   La instancia se visualiza en la ventana **IBM Performance Management**.
4. Pulse el botón derecho del ratón en la instancia de **Monitoring Agent for MariaDB** y pulse **Iniciar**.

   Recuerde: Para configurar el agente de nuevo, complete estos pasos en la ventana de **IBM Performance Management**:

   a. Detenga la instancia de agente que desea configurar.
   b. Pulse el botón derecho del ratón en la instancia de **Monitoring Agent for MariaDB** y pulse **Volver a configurar**.
   c. Repita los pasos 3 y 4.

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener más información sobre la utilización de la Consola de Cloud APM, consulte “Inicio de la Consola de Cloud APM” en la página 1009.

Configuración del agente en sistemas Linux

Puede ejecutar el script de configuración para responder a solicitudes con el fin de configurar el agente en sistemas operativos Linux.

Procedimiento

Para configurar el agente en sistemas operativos Linux, realice los pasos siguientes:

1. En la línea de mandatos, ejecute el siguiente mandato:

   ```
   dir_instalación/bin/mariadb-agent.sh config nombre_instancia
   ```

   Donde *nombre_instancia* es el nombre que desea dar a la instancia y *dir_instalación* es el directorio de instalación del Agente de MariaDB.
2. Cuando se le solicite que especifique un valor para los parámetros siguientes, presione la tecla **Intro** para aceptar el valor predeterminado o especifique otro valor y presione la tecla **Intro**.
   - Dirección IP
   - Nombre de usuario de JDBC
   - Contraseña de JDBC
   - Vuelva a escribir la contraseña de JDBC
   - Archivo .jar de JDBC
   - Número de puerto de JDBC (el número de puerto predeterminado es 3306.)
   - Nivel de rastreo de Java (el valor predeterminado es `Error`).

   Para obtener más información sobre los parámetros de configuración, consulte "Configuración del agente mediante el archivo de respuestas silencioso" en la página 601.
3. Ejecute el mandato siguiente para iniciar el agente:

   ```
   dir_instalación/bin/mariadb-agent.sh start nombre_instancia
   ```

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener más información sobre la utilización de la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

Puede utilizar el archivo de respuestas silencioso para configurar el Agente de MariaDB en sistemas Linux y Windows. Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

Para configurar el agente utilizando el archivo de respuestas silencioso, siga estos pasos:

Recuerde: En este procedimiento se da por supuesto que el agente está instalado en la vía de acceso predeterminada siguiente:

Windows `C:\IBM\APM`

Linux `opt/ibm/apm/agent`

Si el agente se ha instalado en una vía de acceso distinta, sustituya la vía de acceso en las instrucciones. Además, edite el parámetro **AGENT_HOME** en el archivo de respuestas silencioso para especificar la vía de acceso donde se ha instalado el agente.

1. En un editor de texto, abra el archivo de respuestas que está disponible en la siguiente vía de acceso:

   Linux *dir_instalación*/samples/mariadb_silent_config.txt

   Windows *dir_instalación*\samples\mariadb_silent_config.txt

   Donde *dir_instalación* es el directorio de instalación del Agente de MariaDB
2. En el archivo de respuestas, especifique un valor para los parámetros siguientes:
   - Para el parámetro **Nombre de servidor**, especifique la dirección IP de un servidor MariaDB que desea supervisar de forma remota. De lo contrario, retenga el valor predeterminado como `localhost`.
   - Para el parámetro **Nombre de usuario de JDBC**, retenga el valor de nombre de usuario predeterminado `root` o especifique el nombre de un usuario con privilegios para ver las tablas INFORMATION_SCHEMA.
   - Para el parámetro **Contraseña de JDBC**, especifique la contraseña de usuario de JDBC.
   - Para el parámetro **Archivo .jar de JDBC**, retenga la vía de acceso predeterminada si esta vía de acceso al conector MariaDB para el archivo JAR de Java es correcta. De lo contrario, entre la vía de acceso correcta. El conector está disponible en la vía de acceso predeterminada siguiente:

     Linux `/usr/share/java/mariadb-connector-java.jar`

     Windows `C:\Archivos de programa (x86)\MariaDB\mariadb-connector-java.jar`
   - Para el **Número de puerto de JDBC**, retenga el número de puerto predeterminado de 3306 o especifique otro número de puerto.
   - Para el parámetro **Nivel de rastreo de Java**, retenga el valor predeterminado de `Error` o un nivel distinto de acuerdo con las instrucciones del soporte de IBM.
3. Guarde y cierre el archivo de respuestas y ejecute el mandato siguiente para actualizar los valores de configuración del agente:

   Linux *dir_instalación*/bin/mariadb-agent.sh config *nombre_instancia* *dir_instalación*/samples/mariadb_silent_config.txt

   Windows *dir_instalación*\BIN\mariadb-agent.bat config *nombre_instancia* *dir_instalación*\samples\mariadb_silent_config.txt

   Donde *nombre_instancia* es el nombre que desea dar a la instancia y *dir_instalación* es el directorio de instalación del Agente de MariaDB.

   Importante: Asegúrese de incluir la vía de acceso absoluta en el archivo de respuestas silencioso. De lo contrario, los paneles de instrumento no muestran datos de agente.

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener más información sobre la utilización de la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración de la supervisión de Microsoft Active Directory

El Monitoring Agent for Microsoft Active Directory se configura y se inicia automáticamente después de la instalación.

Antes de empezar

Revise los requisitos previos de hardware y software, consulte Software Product Compatibility Reports para el agente de Microsoft Active Directory

Para ver datos para todos los atributos en el panel de instrumentos, realice las siguientes tareas:

- "Ejecución del Agente de Microsoft Active Directory como usuario administrador" en la página 506
- "Configuración de las variables del entorno local" en la página 506

Acerca de esta tarea

Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Ejecución del Agente de Microsoft Active Directory como usuario administrador

Debe tener derechos administrativos para ejecutar el Agente de Microsoft Active Directory.

Acerca de esta tarea

Todos los conjuntos de datos están disponibles para los usuarios que son miembros del grupo Administradores. En esta tarea, creará un usuario, le asignará derechos de administrador y cambiará la cuenta de usuario del agente a este usuario.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Herramientas administrativas** > **Usuarios y equipos de Active Directory**.
2. Para expandir el dominio donde desea crear el usuario, pulse el signo más (+) situado junto al nombre de un dominio.
3. Pulse **Usuarios** con el botón derecho del ratón y, a continuación, pulse **Nuevo** > **Usuario**.
4. Para crear un usuario, abra el asistente **Nuevo objeto - Usuario**.

   De forma predeterminada, un usuario nuevo es miembro del grupo Usuarios de dominio.
5. Pulse el botón derecho del ratón en el nuevo usuario que se crea en el grupo Usuarios del dominio y pulse **Propiedades**. Se visualizará la ventana **Propiedades de nombre de usuario**. El nombre de usuario es el nombre del usuario nuevo.
6. En la ventana **Propiedades de nombre de usuario**, realice los pasos siguientes:
   a) Pulse la pestaña **Miembro de**. En el área **Miembro de**, añada el grupo Administradores.
   b) Pulse **Aplicar** y luego **Aceptar**.
7. Pulse **Inicio** > **Ejecutar** y escriba `services.msc`.
8. En la ventana **Servicios**, realice los pasos siguientes:
   a) Pulse el botón derecho del ratón en el **servicio de Monitoring Agent for Active Directory** y pulse **Propiedades**.
   b) En la ventana **Propiedades de Monitoring Agent for Active Directory**, en la pestaña **Iniciar sesión**, pulse **Esta cuenta**. Especifique las credenciales de usuario.
   c) Pulse **Aplicar** y luego **Aceptar**.
9. Reinicie el servicio de agente.

Configuración de las variables del entorno local

Hay que especificar valores para las variables de entorno para ver los datos de replicación de Sysvol en el panel de instrumentos. De forma opcional, también se puede actualizar el valor del intervalo de caché para habilitar o inhabilitar la caché.

Procedimiento

1. En la ventana **IBM Performance Management**, desde el menú **Acciones** , pulse **Avanzadas** > **Editar archivo ENV**.

2. En el archivo K3ZENV, cambie los valores de las variables de entorno siguientes.

   ADO_CACHE_INTERVAL
   Determina si se inicia o detiene el almacenamiento en caché y se usa para definir un valor de intervalo de caché. El intervalo de caché es el tiempo transcurrido en segundos entre dos recopilaciones de datos consecutivas. Puede especificarse cualquier valor entero positivo en el intervalo de caché para comenzar el almacenamiento en caché. Puede especificarse el valor cero en el intervalo de caché para detener el almacenamiento en caché. De forma predeterminada, se inicia el almacenamiento en caché y el valor de intervalo de caché se establece a 1200.

   ADO_SYSVOL_FORCE_REPLICATION_FLAG
   Determina si la réplica forzada iniciada por el agente se habilita o inhabilita. El valor predeterminado de esta variable es TRUE. Para inhabilitar la réplica forzada, cambie el valor de esta variable a FALSE.

   ADO_SYSVOL_REPLICATION_TEST_INTERVAL
   Determina el intervalo de tiempo en minutos transcurrido entre dos pruebas de replicación de Sysvol. El valor predeterminado de esta variable es de 0 minutos. Para completar la prueba de replicación de Sysvol, asegúrese de que el valor de esta variable sea mayor que cero.

   ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL
   Determina el tiempo en minutos que el agente espera para verificar los resultados de replicación de Sysvol una vez completada la prueba de replicación de Sysvol.

   El valor de la variable **ADO_SYSVOL_REPLICATION_TEST_INTERVAL** debe ser mayor que el valor de la variable **ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL**. Puede utilizar los siguientes valores para estas variables:

   ADO_SYSVOL_REPLICATION_TEST_INTERVAL: 1440
   ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL: 30

   Después de asignar valores válidos a las variables de entorno, el agente de Active Directory crea un archivo en la carpeta compartida Sysvol del sistema gestionado e inicializa la réplica forzada de Sysvol. Esta réplica forzada se inicializa desde el sistema gestionado en las carpetas compartidas Sysvol de los asociados de réplica Sysvol. Después de verificar los resultados de la prueba de réplica, el agente elimina los archivos creados y gestionados desde el sistema gestionado y los asociados de réplica de Sysvol.
3. Opcional: En el archivo K3ZENV, añada la variable de entorno **APM_ATTRIBUTES_ENABLE_COLLECTION** y establezca su valor en Yes para ver los datos de los siguientes conjuntos de datos en la pestaña **Detalles de atributo**.

   - Servicios
   - Réplica
   - Servicio de réplica de archivos
   - Unidad organizativa movida o suprimida
   - LDAP
   - Gestor de cuentas de seguridad
   - DFS
   - Libreta de direcciones
   - Registro de sucesos
   - Objetos de establecimiento de contraseña

   Recuerde: si desea inhabilitar la recopilación de datos para estos conjuntos de datos, establezca el valor de la variable de entorno **APM_ATTRIBUTES_ENABLE_COLLECTION** en No.
4. Reinicie el Agente de Microsoft Active Directory.

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Ejecución de Agente de Microsoft Active Directory como usuario no administrador

Puede ejecutar el Agente de archivo de registro como usuario no administrativo.

Acerca de esta tarea

Puede ejecutar el agente de supervisión para Active Directory como usuario no administrador; sin embargo, es posible que los atributos de Topología de Trust y los atributos de Réplica de Sysvol no estén disponibles. Estos atributos sólo están disponibles para usuarios de dominio.

Para ver los atributos de Topología de Trust, un usuario no administrador debe tener los permisos de registro siguientes:

- Otorgue acceso completo al directorio `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`.
- Otorgue acceso de lectura al directorio `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Perflib`.

Para ver los atributos de Réplica de Sysvol, un usuario no administrador debe tener acceso completo a la carpeta `Sysvol` en todos los controladores de dominio de un dominio.

Importante: cuando Agente de Microsoft Active Directory se ejecuta como un usuario no administrador, algunos servicios del grupo de atributos Servicios muestran los valores de los atributos Estado actual y Tipo de inicio como Desconocido en la interfaz de usuario de APM.

La tabla siguiente contiene los grupos de atributos para el agente de Active Directory que muestra los datos para los usuarios de dominio y para los usuarios de la supervisión de rendimiento.

Tabla 171. Grupos de atributos para los usuarios de dominio y los usuarios de supervisión de rendimiento.

Derecho de usuario	Grupo de atributos
Usuarios de dominio	• Información de la agrupación de RID • Servicios • Registros de sucesos • DNS • Detalles de DNS ADIntegrated • DNS ADIntegrated • DHCP • Confianza • Objetos de política de grupo • Objetos perdidos y encontrados • Servicio de directorio de Exchange • Objetos Conflicto de replicación • Atributo LDAP • Servidor de directorios raíz • Contenedores • Asociado de réplica • Disponibilidad del controlador de dominio • Latencia de asociado de réplica • Topología de bosque

Tabla 171. Grupos de atributos para los usuarios de dominio y los usuarios de supervisión de rendimiento. (continuación)

Derecho de usuario	Grupo de atributos
Usuarios de dominio y usuarios de supervisión de rendimiento.	Todos los grupos de atributos que se mencionan para los usuarios de dominio y los siguientes grupos de atributos adicionales: • Libreta de direcciones • Réplica • Servicios de directorio • Knowledge Consistency Checker • Centro de distribución de claves Kerberos • Lightweight Directory Access Protocol • Autoridad de seguridad local • Proveedor de servicio de nombres • Gestor de cuentas de seguridad • Servicio de réplica de archivos • Réplica del sistema de archivos distribuido • Conexiones de réplica DFS • Carpetas de réplica DFS • Volumen de servicio DFS • Rendimiento del controlador de dominio • Servidor de acceso remoto • Servidor de acceso directo • Atributos de Netlogon

Nota: Además, los grupos de atributos siguientes muestran datos para los usuarios que son miembros del grupo de *administradores*:

- Información de la base de datos de Active Directory
- Unidad organizativa movida o suprimida
- Objetos de establecimiento de contraseña

Para obtener información, consulte "Configuración de la supervisión de Microsoft Active Directory" en la página 505

Procedimiento

1. Pulse **Inicio>Programas>Herramientas administrativas>Usuarios y equipos de Active Directory**.
2. Expanda el dominio en el que desea crear el usuario pulsando el signo más (+) junto al nombre de un dominio.
3. Pulse **Usuarios** con el botón derecho del ratón y, a continuación, pulse **Nuevo>Usuario**.
4. Cree un nuevo usuario utilizando el asistente **Nuevo Objeto - Usuario**. De forma predeterminada, un usuario nuevo es miembro del grupo **Usuarios de dominio**.
5. Pulse el botón derecho del ratón en el nuevo usuario que se crea en el grupo *Usuarios del dominio* y pulse **Propiedades**. Se abrirá la ventana **Propiedades de nombre de usuario**, donde *nombre de usuario* es el nombre del usuario nuevo. Realice los pasos siguientes en la ventana **Propiedades de nombre de usuario**:
   a) Pulse el separador **Miembro de**. En el área **Miembro de**, añada el grupo **Usuarios de supervisor de rendimiento**.

b) Pulse **Aplicar** y luego **Aceptar**.

6. Vaya al directorio `Inicio_Candle`. La vía de acceso predeterminada es `C:\IBM\APM`.
7. Pulse la carpeta APM con el botón derecho del ratón y pulse **Propiedades**. Se abrirá la ventana **Propiedades de APM**. Complete los pasos siguientes en la ventana **Propiedades APM**:
   a) En la pestaña **Seguridad**, pulse **Editar**.
   b) Pulse **Añadir** para añadir el usuario nuevo y otorgue acceso completo a este usuario.
   c) Pulse **Aplicar** y luego **Aceptar**.
8. Pulse **Inicio > Ejecutar** y escriba `services.msc`. Se abrirá la ventana **Servicios**. Complete los pasos siguientes en la ventana **Servicios**:
   a) Pulse el botón derecho del ratón en el servicio **Agente de supervisión** para Active Directory y pulse **Propiedades**.
   b) En la ventana **Propiedades de Active Directory**, en el separador **Iniciar sesión**, pulse **Esta cuenta**. Especifique las credenciales de usuario.
   c) Pulse **Aplicar** y luego **Aceptar**.
9. Reinicie el servicio de agente.

Configuración de servicios de dominio para el grupo de atributos AD_Services_Status

Puede configurar los servicios de dominio de MS Active Directory en `Services.properties` para que se utilicen o se excluyan
al determinar el `Estado del servidor`. El grupo de atributos `AD_Services_Status` y su situación son aplicables a
Windows Server 2012 y posteriores.

Acerca de esta tarea

El archivo `Services.properties` contiene los siguientes servicios de dominio predeterminados de MS Active Directory y su configuración.
True indica que el servicio se tendrá en cuenta al determinar el valor de Estado del servidor.
False indica que el servicio no se tendrá en cuenta al determinar el valor de Estado del servidor.

Tabla 172. Servicios de dominio de MS Active Directory y valor de configuración.

Servicios de dominio de MS Active Directory	**Valor predeterminado**
Réplica de DFS	true
Llamada de procedimiento remoto (RPC)	false
Cliente DNS	true
Servidor DNS	true
Cliente de política de grupo	false
Mensajería entre sitios	true
Centro de distribución de claves Kerberos	true
NetLogon	true
Hora de Windows	true
Cliente de DHCP	false
Servicios web de Active Directory	false
Servicios de federación de Active Directory	false

Nota: es necesario reiniciar el agente para habilitar la recopilación de datos para el grupo de atributos `AD_Services_Status` en Windows Server 2012 y posteriores.

Procedimiento

1. Detenga el agente.
2. Localice el archivo `Services.properties` para modificarlo, si es necesario.
   Para el agente de 32 bits, el archivo `Services.properties` se encuentra en *INICIO_CANDLE* `\TMAITM6\`.
   Para el agente de 64 bits, el archivo `Services.properties` se encuentra en *INICIO_CANDLE* `\TMAITM6_x64\`.
   INICIO_CANDLE es el directorio de instalación del agente.
3. Si desea que los servicios de dominio se tengan en cuenta al determinar el estado del servidor, establezca su valor en true.
   Si desea excluir los Servicios de dominio al determinar el estado del servidor, establezca su valor en false.
   Guarde los cambios y cierre el archivo.
4. Inicie el agente.

Actualización de Agente de Microsoft Active Directory

Puede actualizar el agente de MS Active Directory a la última versión.

Antes de empezar

Asegúrese de que el archivo `installAPMAgents.bat` proporcionado en el instalador del último release está disponible en la máquina en la que está instalado el agente.

Acerca de esta tarea

Para actualizar el agente a la versión más reciente, complete el procedimiento siguiente.

Procedimiento

1. Inicie la sesión en la máquina en la que está instalado el agente.
2. Inicie un indicador de mandatos, ejecute el archivo `installAPMAgents.bat` cuyo origen está en el instalador del último release.
3. Especifique el directorio de instalación en el que reside el agente existente y pulse Intro.
4. El indicador de mandatos muestra la versión de agente base y la versión de agente de destino que se deben actualizar. Pulse Intro para continuar.
5. Cuando la actualización de agente se realiza satisfactoriamente, se muestra la versión de agente actualizada en la ventana **IBM Performance Management**.
6. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en el agente y seleccione **Reconfigurar** en el menú desplegable.
7. Para reflejar la versión de agente actualizada en el **Panel de instrumentos del rendimiento de aplicaciones**, inicie la sesión en el servidor APM y reinicie los componentes de servidor APM utilizando los mandatos siguientes.
   a. **`apm stop_all`**
   b. **`apm start_all`**
8. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en el agente y seleccione **Reciclar** en el menú desplegable.

Resultados

El agente actualizado se refleja en el **Panel de instrumentos del rendimiento de aplicaciones**.

Nota: Puede que se necesiten 30 minutos o más para mostrar el agente actualizado en el **Panel de instrumentos del rendimiento de aplicaciones**.

Configuración de la supervisión de Microsoft Cluster Server

Debe configurar el Monitoring Agent for Microsoft Cluster Server para que el agente pueda recopilar los datos del servidor de clúster. Utilice el archivo de respuestas silencioso para configurar el agente.

Antes de empezar

Asegúrese de que completa las tareas siguientes:

- Cree un grupo de recursos vacío para el agente.
- Cree un recurso de clúster de servicio genérico en el grupo de recursos del agente en los sistemas Windows Server 2008, 2012, 2016 y 2019.
- Asegúrese de que el usuario que se conecta al entorno o a la aplicación de Microsoft Cluster Server tiene privilegios de administrador. Utilice un usuario existente con privilegios de administrador, o cree un nuevo usuario. Asigne privilegios de administrador al nuevo usuario añadiendo el nuevo usuario al grupo Administradores.

  Recuerde: Para configurar Agente de Microsoft Cluster Server, puede utilizar un usuario de dominio o local siempre que el usuario tenga privilegios de administrador.

Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Microsoft Cluster Server.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte “Historial de cambios” en la página 52.

Acerca de esta tarea

Agente de Microsoft Cluster Server es un agente de instancia única. Debe instalar y configurar el agente manualmente del mismo modo en todos los nodos del clúster. Para configurar el agente, consulte “Configuración del agente mediante el archivo de respuestas silencioso” en la página 514.

Creación de un recurso de clúster de servicio genérico en los sistemas Windows Server 2008, 2012, 2016 y 2019

Debe añadir el servicio de agente de clúster como un recurso de modo que el agente pueda supervisar el servidor de clúster.

Antes de empezar

Asegúrese de que se detiene el agente en todos los nodos del clúster.

Procedimiento

Para crear un recurso de clúster de servicio genérico, realice los pasos siguientes:

1. Abra el **Administrador de clústeres de conmutación por error** en cualquiera de los nodos de clúster.
2. Complete uno de los pasos siguientes:
   - Para Windows Server 2008:

     En el panel de navegación, pulse el botón derecho del ratón en **Servicios y aplicaciones** y, a continuación, pulse **Más acciones** > **Crear servicio o aplicación vacíos**. El nuevo servicio se mostrará en la lista de servicios y aplicaciones. Renombre el servicio que acaba de crear.
   - En Windows Server 2012:

     En el panel de navegación, pulse el botón derecho del ratón en **Roles** y, a continuación, pulse **Más acciones** > **Crear roles**. El nuevo servicio se visualizará en la lista de roles.

- Para Windows Server 2016 y 2019:

  En el panel de navegación, pulse con el botón derecho del ratón en **Roles** y, a continuación, pulse **Configurar roles**. Se visualizará el nuevo servicio.

3. Pulse el botón derecho (del ratón) en el nuevo servicio y pulse **Añadir recurso** > **Servicio genérico**.
4. En la ventana del asistente **Nuevo recurso**, seleccione **Monitoring Agent for Microsoft Cluster Server** y pulse **Siguiente**.
5. Pulse **Siguiente** en las ventanas subsiguientes hasta que vea el botón **Finalizar**.
6. Pulse **Finalizar**.

   El servicio de agente se añadirá como recurso.
7. Pulse en el recurso **Monitoring Agent for Microsoft Cluster Server** y pulse **Situar el recurso en línea**.

Resultados
Se iniciará el agente en el nodo preferido.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del Agente de Microsoft Cluster Server con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para configurar los diferentes valores de los parámetros de configuración del agente.

Antes de empezar

Cree un archivo de respuesta que contenga los parámetros de configuración que desea modificar. Si desea modificar los parámetros de configuración predeterminados, edite el archivo de respuestas.

Acerca de esta tarea
Puede configurar el agente utilizando el archivo de respuestas silencioso.

Procedimiento

1. Abra el archivo de respuestas silencioso que está disponible en esta vía de acceso: *dir_instalación*\samples\microsoft_cluster_server_silent_config.txt
2. Para la variable de entorno **CTIRA_HOSTNAME**, especifique el nombre de clúster como un valor.
3. En cada nodo de clúster, ejecute el mandato siguiente: **dir_instalación\BIN \microsoft_cluster_server-agent.bat config dir_instalación\samples \microsoft_cluster_server_silent_config.txt**

Qué hacer a continuación
Cambie la cuenta de usuario del usuario local por el usuario de dominio.

Cambio de la cuenta de usuario

Después de configurar Agente de Microsoft Cluster Server, puede cambiar la cuenta de usuario del usuario local al usuario de dominio.

Acerca de esta tarea
De forma predeterminada, el agente se ejecuta bajo la cuenta de usuario local. El agente se debe ejecutar bajo el usuario de dominio de modo que el agente pueda supervisar todos los nodos del clúster desde un nodo único.

Procedimiento

Para cambiar la cuenta de usuario, realice los pasos siguientes:

1. Abra la ventana **IBM Performance Management**.
2. Pulse el botón derecho (del ratón) en el agente y, a continuación, pulse **Cambiar inicio**.

3. Entre las credenciales de inicio de sesión de dominio.
4. Abra el **Administrador de clústeres de conmutación por error** en uno de los nodos e inicie el servicio de clúster.

Resultados
Se iniciará el agente en el nodo.

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información acerca de cómo usar la consola de Performance Management, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración de la supervisión de Microsoft Exchange

Debe configurar el Monitoring Agent for Microsoft Exchange Server para supervisar la disponibilidad y el rendimiento de los servidores Exchange Server.

Antes de empezar
Antes de configurar el agente, asegúrese de que haya completado las tareas siguientes:

- "Creación de usuarios" en la página 515
- "Asignación de derechos de administrador al usuario de Exchange Server" en la página 518
- "Cómo convertir el usuario de Exchange Server en un administrador local" en la página 520
- "Configuración de Exchange Server para la accesibilidad" en la página 521
- "Configuración del agente que se ejecutará en el usuario de dominio" en la página 522
- Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Microsoft Exchange Server.

Acerca de esta tarea

Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Puede iniciar el Agente de Microsoft Exchange Server después de que se ha instalado el agente. Sin embargo, es necesaria la configuración manual para ver los datos de todos los atributos de agente.

- Para configurar el agente localmente, consulte "Configuración del agente localmente" en la página 523.
- Para configurar el agente mediante el archivo de respuestas silencioso, consulte "Configuración del agente mediante el archivo de respuestas silencioso" en la página 527.

Creación de usuarios

Puede crear un usuario para el agente en Exchange Server de forma manual o ejecutando el programa de utilidad *Nuevo usuario*. Debe crear el usuario en cada Exchange Server que desee supervisar.

Antes de empezar
Instale el Agente de Microsoft Exchange Server. Para crear un usuario, debe ser un administrador de dominios con derechos de administrador completos en Microsoft Exchange Server.

Acerca de esta tarea

Utilice uno de los procedimientos siguientes para crear usuarios:

Creación de usuarios en Exchange Server 2007 y 2010

Debe crear un usuario para el agente en Exchange Server 2007 y 2010 para que el agente pueda comunicarse y autenticarse con el Exchange Server que desea supervisar.

Procedimiento

Para crear un usuario, realice los pasos siguientes:

1. Pulse **Inicio > Programas > Microsoft Exchange Server 2007 > Consola de administración de Exchange**. Se abrirá la ventana **Consola de administración de Exchange**.
2. En el árbol de la consola, pulse **Configuración de destinatario de buzón**.
3. En el panel de Acciones, pulse **Nuevo buzón**. Se abre el asistente de nuevo buzón.
4. En la página **Introducción**, pulse **Buzones de usuario**.
5. En la página **Tipo de usuario**, pulse **Nuevo usuario**.
6. En la página **Información de usuario**, especifique la información siguiente:

   Unidad organizativa
   De forma predeterminada, se muestra el contenedor de usuarios en Active Directory. Pulse **Examinar** para cambiar el valor predeterminado de la unidad organizativa.

   Nombre
   Escriba el nombre del usuario.

   Iniciales
   Escriba las iniciales del usuario.

   Apellidos
   Escriba los apellidos del usuario.

   Nombre
   De forma predeterminada, en este campo se muestra el nombre, las iniciales y el apellido del usuario. Puede modificar el nombre.

   Nombre de usuario de inicio de sesión (nombre principal de usuario)
   Escriba el nombre que el usuario debe utilizar para iniciar la sesión en el buzón.

   Nombre de inicio de sesión de usuario (anterior a Windows 2000)
   Escriba el nombre de usuario que sea compatible con Microsoft Windows 2000 Server o anterior.

   Contraseña
   Escriba la contraseña que el usuario debe utilizar para iniciar la sesión en el buzón.

   Confirmar contraseña
   Vuelva a escribir la contraseña que ha especificado en el campo **Contraseña**.

   El usuario debe cambiar la contraseña en el siguiente inicio de sesión.
   Seleccione este recuadro si desea que el usuario restablezca la contraseña.
7. En la página **Configuración del buzón**, especifique la información siguiente:

   Alias
   De forma predeterminada, el valor de este campo es idéntico al valor especificado en el campo **Nombre de inicio de sesión de usuario (Nombre principal de usuario)**.

   Base de datos de buzón
   Pulse en **Examinar** para abrir la ventana **Seleccionar base de datos de buzones de correo**. Seleccione la base de datos de buzón que desea utilizar y pulse **Aceptar**.

   Política de buzón de carpetas gestionadas
   Seleccione este recuadro de selección para especificar una política de gestión de registros de mensajería (directiva MRM). Pulse **Examinar** para seleccionar la política de buzón MRM que desea asociar a este buzón.

Política de buzón de Exchange ActiveSync
Seleccione este recuadro de selección para especificar una política de buzón de Exchange ActiveSync. Pulse **Examinar** para seleccionar la política de buzón de Exchange ActiveSync que desea asociar a este buzón.

8. En la página **Nuevo buzón**, revise el resumen de configuración. Pulse **Nuevo** para crear un buzón. En la página **Finalización**, la sección Resumen muestra si el buzón se ha creado.
9. Pulse **Finalizar**.

Qué hacer a continuación

Asigne derechos de administrador al usuario de Exchange que ha creado.

Creación de usuarios en Exchange Server 2013
Debe crear un usuario para el agente en Exchange Server 2013 para que el agente pueda comunicarse y autenticarse con el Exchange Server que desea supervisar.

Procedimiento

Para crear un usuario en Exchange Server 2013, siga estos pasos:

1. Inicie la sesión en el centro de administración de Exchange con las credenciales de administrador.
2. En la página **Centro de administrador de Exchange**, pulse **destinatarios** y luego pulse **buzones**.
3. Pulse la flecha hacia abajo al lado del signo más (+) que está debajo de la opción **buzones** y luego pulse **Buzón de usuario**.
4. En la página "Buzón de nuevo usuario", pulse **Nuevo usuario** y especifique los valores de otros campos.
5. Pulse **Guardar**.

Qué hacer a continuación

Asigne derechos de administrador al usuario de Exchange que ha creado.

Creación de usuarios ejecutando el programa de utilidad Nuevo usuario
Puede ejecutar el programa de utilidad Nuevo usuario para crear usuarios en Exchange Server 2007 o posterior. El usuario que se crea mediante la ejecución de este programa de utilidad tiene todos los permisos necesarios para ejecutar el agente. Este programa de utilidad se instala al instalar el agente.

Antes de empezar
Asegúrese de que está instalado el agente. Para ejecutar el programa de utilidad Nuevo usuario, debe ser un administrador de dominios con derechos de administrador completos en Exchange Server.

Acerca de esta tarea
Cuando ejecuta este programa de utilidad, el usuario se crea en el grupo Usuarios de Active Directory, y tiene los permisos siguientes:

- En Exchange Server 2007:
  - Administrador local
  - Usuario de escritorio remoto
  - Administrador de destinatarios de Exchange
- En Exchange Server 2010 o posterior:
  - Administrador local
  - Usuario de escritorio remoto
  - Exchange Servers or Public Folder Management.

Procedimiento

Para ejecutar el programa de utilidad Nuevo usuario, realice los pasos siguientes:

1. Efectúe una doble pulsación en el archivo `kexnewuser.exe` que está disponible en la siguiente ubicación:

   dir_instal\TMAITM6_x64, donde *dir_instal* es la vía de acceso donde está instalado el agente.
2. En la ventana **Nuevo usuario**, complete los siguientes pasos:
   a) Especifique el **nombre** y **apellido** del usuario.

      Restricción: La longitud del nombre y apellido no debe superar los 28 caracteres.

   b) En el campo **Nombre de inicio de sesión de usuario**, escriba el nombre que el usuario debe escribir al iniciar sesión.

      Restricción: La longitud del nombre de inicio de sesión de usuario no debe superar los 256 caracteres.

   c) En el campo **Contraseña**, escriba su contraseña.

   d) En el campo **Confirmar contraseña**, especifique de nuevo la contraseña.

   e) Seleccione **El usuario debe cambiar la contraseña en el siguiente inicio de sesión** si desea que la contraseña especificada se restablezca cuando el usuario inicie sesión.

   f) Pulse **Siguiente**.

   Se validarán los valores de configuración especificados y se visualizarán mensajes de error para los valores incorrectos.
3. En la lista de bases de datos de buzón, seleccione la base de datos de buzón necesaria y pulse **Siguiente**.

   Se mostrará un resumen de valores de configuración.
4. Pulse **Finalizar**.

Resultados

Se guardarán los valores y se creará el usuario.

Asignación de derechos de administrador al usuario de Exchange Server

El usuario creado para el Agente de Microsoft Exchange Server debe ser administrador de dominios con plenos derechos de administrador sobre Microsoft Exchange Server. Los derechos de administrador son necesarios para acceder a los componentes de Agente de Microsoft Exchange Server.

Antes de empezar

Cree un usuario de Exchange Server que tenga el buzón en el Exchange Server que se está supervisando.

Acerca de esta tarea

Utilice uno de los procedimientos siguientes para asignar derechos de administrador al usuario:

- "Asignación de derechos de administrador en Exchange Server 2007" en la página 518
- "Asignación de derechos de administrador en Exchange Server 2010" en la página 519
- "Asignación de derechos de administrador en Exchange Server 2013" en la página 519
- "Asignación de derechos de administrador en Exchange Server 2016" en la página 519

Asignación de derechos de administrador en Exchange Server 2007

Debe asignar derechos de administrador de destinatarios de Exchange al usuario en el Exchange Server 2007.

Procedimiento

1. Pulse **Inicio > Programas > Microsoft Exchange > Usuarios y equipos de Exchange Server 2007 > Consola de administración de Exchange**. Se abrirá la ventana **Consola de administración de Exchange**.
2. En el árbol de la consola, pulse **Configuración de la organización**.
3. En el panel de Acciones, pulse **Añadir administrador de Exchange**.
4. En la página **Añadir administrador de Exchange**, pulse **Examinar**. Seleccione el nuevo usuario que ha creado y luego seleccione el rol **Administrador de destinatarios de Exchange**.
5. Pulse **Añadir**.
6. En la página **Finalización**, pulse **Finalizar**.

Asignación de derechos de administrador en Exchange Server 2010
Debe asignar los derechos Exchange Servers or Public Folder Management al usuario en Exchange Server 2010.

Procedimiento

1. Inicie sesión en el servidor Exchange con privilegios de administrador.
2. Pulse **Inicio > Herramientas administrativas > Server Manager**.
3. Expanda **Herramientas**.
4. Pulse **Usuarios y equipos de Active Directory**.
5. Expanda **Dominio** y pulse **Grupos de seguridad de Microsoft Exchange**.
6. Pulse **Exchange Servers or Public Folder Management** con el botón derecho del ratón y, a continuación, pulse **Propiedades**.
7. En la ventana **Propiedades de Exchange Servers o Propiedades de Public Folder Management**, vaya a **Miembros** y pulse **Agregar**.
8. Desde la lista de usuarios, seleccione el usuario que desea añadir al grupo y pulse **Aceptar**.
9. Pulse **Aceptar**.

Asignación de derechos de administrador en Exchange Server 2013
Debe asignar los derechos Exchange Servers or Public Folder Management al usuario en Exchange Server 2013.

Procedimiento

1. Inicie sesión en Exchange Server con privilegios de administrador.
2. Pulse **Inicio > Herramientas administrativas > Server Manager**.
3. Expanda **Herramientas**.
4. Pulse **Usuarios y equipos de Active Directory**.
5. Expanda **Dominio** y pulse **Grupos de seguridad de Microsoft Exchange**.
6. Pulse **Exchange Servers or Public Folder Management** con el botón derecho del ratón y, a continuación, pulse **Propiedades**.
7. En la ventana **Propiedades de Exchange Servers o Propiedades de Public Folder Management**, vaya a **Miembros** y pulse **Agregar**.
8. Desde la lista de usuarios, seleccione el usuario que desea añadir al grupo y pulse **Aceptar**.
9. Pulse **Aceptar**.

Asignación de derechos de administrador en Exchange Server 2016
Debe asignar los derechos Exchange Servers or Public Folder Management al usuario en Exchange Server 2016.

Procedimiento

1. Inicie sesión en Exchange Server con privilegios de administrador.
2. Pulse **Inicio > Herramientas administrativas > Server Manager**.
3. Expanda **Herramientas**.
4. Pulse **Usuarios y equipos de Active Directory**.
5. Expanda **Dominio** y pulse **Grupos de seguridad de Microsoft Exchange**.
6. Pulse **Exchange Servers or Public Folder Management** con el botón derecho del ratón y, a continuación, pulse **Propiedades**.
7. En la ventana **Propiedades de Exchange Servers o Propiedades de Public Folder Management**, vaya a **Miembros** y pulse **Agregar**.
8. Desde la lista de usuarios, seleccione el usuario que desea añadir al grupo y pulse **Aceptar**.
9. Pulse **Aceptar**.

Qué hacer a continuación
Convierta el usuario en un administrador local del sistema en el que se ha instalado Exchange Server.

Cómo convertir el usuario de Exchange Server en un administrador local

Para acceder a los datos de Exchange Server, el usuario que ha creado para el Agente de Microsoft Exchange Server deberá ser un administrador local del sistema donde esté instalado Exchange Server.

Antes de empezar
Cree un usuario de Exchange Server

Acerca de esta tarea
Utilice uno de los procedimientos siguientes para convertir el usuario en un administrador local:

- “Cómo convertir el usuario en un administrador local en Windows 2003” en la página 520
- “Cómo convertir el usuario en un administrador local en Windows 2008” en la página 520
- “Cómo convertir el usuario en un administrador local en Windows 2012” en la página 521
- “Cómo convertir el usuario en un administrador local en Windows 2016” en la página 521

Cómo convertir el usuario en un administrador local en Windows 2003
Debe convertir el usuario que ha creado para Exchange Server en un administrador local del sistema que ejecuta el sistema operativo Windows 2003 y donde Exchange Server se ha instalado.

Procedimiento

1. Pulse con el botón derecho de ratón en **Mi PC** en el escritorio del sistema y pulse en **Administrar**.
2. Expanda **Usuarios locales y grupos**.
3. Pulse **Grupos**.
4. Efectúe una doble pulsación en **Administradores** para visualizar la ventana **Propiedades de Administradores**.
5. Pulse **Añadir**.
6. Seleccione **El directorio completo** en la lista **Buscar en**.
7. Seleccione el nombre del usuario que ha creado y pulse en **Agregar**.
8. Pulse **Aceptar**.
9. Pulse **Aceptar**.

Cómo convertir el usuario en un administrador local en Windows 2008
Debe convertir el usuario que ha creado para Exchange Server en un administrador local del sistema que ejecuta el sistema operativo Windows Server 2008 y donde Exchange Server se ha instalado.

Procedimiento

1. Pulse **Inicio > Herramientas administrativas > Server Manager**.
2. En el panel de navegación, expanda **Configuración**.
3. Efectúe una doble pulsación en **Usuarios y grupos locales**.
4. Pulse **Grupos**.
5. Pulse con el botón derecho del ratón en el grupo al que desea añadir la cuenta de usuario y, a continuación, pulse **Añadir a grupo**.
6. Pulse **Añadir** y escriba el nombre de la cuenta de usuario.
7. Pulse **Comprobar nombres** y, a continuación, pulse **Aceptar**.

Cómo convertir el usuario en un administrador local en Windows 2012
Debe convertir el usuario que ha creado para Exchange Server en un administrador local del sistema que ejecuta el sistema operativo Windows Server 2012 y donde se ha instalado Exchange Server.

Procedimiento

1. Pulse **Inicio > Server Manager**.
2. En la esquina superior derecha del **Panel de instrumentos de Server Manager**, pulse **Herramientas > Administración de equipos**.
3. En el panel de navegación de la página **Administración de equipos**, expanda **Usuarios locales y grupos** y pulse **Usuarios**.
4. En la lista de usuarios, pulse el botón derecho del ratón en el usuario al que desea asignar derechos administrativos y pulse **Propiedades**.
5. Pulse el separador **Miembro de** y luego pulse en **Añadir**.
6. En la página **Seleccionar grupo**, escriba `Administradores` y luego en **Aceptar**.
7. Pulse **Aplicar** y **Aceptar**.

Cómo convertir el usuario en un administrador local en Windows 2016
Debe convertir el usuario que ha creado para Exchange Server en un administrador local del sistema que ejecuta el sistema operativo Windows Server 2016 y donde se ha instalado Exchange Server.

Procedimiento

1. Pulse **Inicio > Server Manager**.
2. En la esquina superior derecha del **Panel de instrumentos de Server Manager**, pulse **Herramientas > Administración de equipos**.
3. En el panel de navegación de la página **Administración de equipos**, expanda **Usuarios locales y grupos** y pulse **Usuarios**.
4. En la lista de usuarios, pulse el botón derecho del ratón en el usuario al que desea asignar derechos administrativos y pulse **Propiedades**.
5. Pulse el separador **Miembro de** y luego pulse en **Añadir**.
6. En la página **Seleccionar grupo**, escriba `Administradores` y luego en **Aceptar**.
7. Pulse **Aplicar** y **Aceptar**.

Configuración de Exchange Server para la accesibilidad

Para verificar la posibilidad de alcance, el Agente de Microsoft Exchange Server envía un mensaje de correo electrónico al servidor y mide la cantidad de tiempo que lleva recibir una respuesta automática. Antes de iniciar el agente, debe configurar Exchange Server para que responda automáticamente a los mensajes de correo electrónico.

Antes de empezar
Antes de configurar Exchange Server, asegúrese de que se han completado las tareas siguientes:

- Se crea un buzón para el usuario en el Exchange Server que desea supervisar.
- El usuario que ha creado para el agente es un usuario de dominio.
- Los servidores de la organización de Microsoft Exchange están configurados para el flujo de correo entre servidores.

Procedimiento

Complete los pasos siguientes para todos los Exchange Server para los que desea verificar la accesibilidad:

1. Inicie sesión en Microsoft Outlook especificando las credenciales del usuario que ha creado.
2. Pulse en **Siguiente** en la ventana **Inicio**.
3. Seleccione **Sí** y pulse en **Siguiente**.
4. En el campo **Microsoft Exchange Server**, escriba el nombre del Exchange Server.
5. En el campo **Buzón**, escriba el nombre del usuario que ha creado.
6. Pulse **Finalizar**.
7. Pulse **Aceptar**.
8. Pulse en **Herramientas > Reglas y alertas > Nueva regla**.
9. Seleccione **Iniciar desde una regla en blanco**.
10. Seleccione **Comprobar los mensajes cuando lleguen** y pulse en **Siguiente**.
11. Seleccione las opciones siguientes:
    - **donde mi nombre aparezca en el cuadro Para:**
    - **con cierto texto en el asunto o en el cuerpo del mensaje**
12. En el **Paso 2** de la ventana, pulse en **cierto texto**.
13. En el campo **Especifique las palabras o frases que desee buscar en el asunto o cuerpo del mensaje**, escriba `AVAILABILITY CHECK`.
14. Pulse **Añadir**.
15. Pulse **Aceptar** y, a continuación, pulse **Siguiente**.
16. Seleccione **disponer de respuesta del servidor mediante un mensaje determinado** y pulse en **un mensaje determinado**.
17. En el editor de mensajes de correo electrónico, escriba el texto siguiente en el campo de asunto del mensaje:

    ```
    CHECK RECEIVED: MAILBOX AVAILABLE.
    ```
18. Cierre el editor de mensajes de correo electrónico y pulse **Sí** para guardar estos cambios.
19. Pulse **Siguiente**.
20. Cuando le pregunten sobre excepciones, no especifique ninguna restricción.
21. Pulse **Siguiente**.
22. Pulse **Finalizar** y luego **Aceptar**.

Qué hacer a continuación

Configure el Agente de Microsoft Exchange Server.

Configuración del agente que se ejecutará en el usuario de dominio

De forma predeterminada, el Agente de Microsoft Exchange Server está configurado para ejecutarse bajo el usuario local. El agente debe ejecutarse bajo el usuario de dominio que ha creado.

Antes de empezar

Asegúrese de lo siguiente:

- El usuario que ha creado es un usuario de dominio con los derechos de administrador local.
- El usuario tiene derechos de administrador en el servidor donde está instalado el agente.

Acerca de esta tarea
Cuando el agente se ejecuta bajo el usuario de dominio, el agente puede supervisar todos los componentes del Exchange Server.

Procedimiento

Para cambiar el usuario bajo el que se ejecuta el agente, realice los pasos siguientes:

1. Ejecute el mandato siguiente para verificar qué ID de usuario se utiliza para iniciar el agente.
   `dir_instalación\InstallITM\KinCinfo.exe -r`
2. Si el agente de supervisión se ha iniciado con un ID de usuario que no pertenece al grupo Administrador, detenga el agente.
3. Abra la ventana **Gestionar servicios de supervisión**.
4. Pulse con el botón derecho en la instancia de agente y, a continuación, pulse **Cambiar inicio**.
5. Especifique el ID de usuario totalmente calificado como `<Dominio\ID de usuario>` y, a continuación, especifique la contraseña.
6. Inicie el agente de supervisión.

Configuración del agente localmente

Puede configurar el agente localmente utilizando la ventana IBM Cloud Application Performance Management.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en **Monitoring Agent for Microsoft Exchange Server** y luego pulse **Configurar agente**.

   Atención: Pulse **Reconfigurar** si **Configurar agente** está inhabilitado.
3. En la ventana **Monitoring Agent for Microsoft Exchange Server: Configuración avanzada de agente**, pulse **Aceptar**.
4. En la ventana **Configuración de agente**, complete los siguientes pasos:
   a) Pulse la pestaña **Propiedades de Exchange Server** y especifique valores para parámetros de configuración. Cuando pulse **Aceptar**, se validarán los valores especificados.
   b) Pulse la pestaña **Supervisión de servicios de Exchange** y especifique los valores para parámetros de configuración. Cuando pulse **Aceptar**, se validarán los valores especificados.
   c) Pulse la pestaña **Propiedades de configuración avanzadas** y especifique valores para parámetros de configuración. Cuando pulse **Aceptar**, se validarán los valores especificados.

   Para obtener información sobre los parámetros de configuración en cada pestaña de la ventana **Configuración del agente**, consulte los temas siguientes:

   - “Parámetros de configuración para las propiedades de Exchange Server” en la página 524
   - “Parámetros de configuración de los servicios de Exchange” en la página 525
   - “Parámetros de configuración para la accesibilidad” en la página 526

   Para obtener información acerca de la validación de valores de configuración, consulte “Validación de valores de configuración” en la página 527.
5. Reinicie el agente.

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte “Inicio de la Consola de Cloud APM” en la página 1009.

Restricción: En el panel de instrumentos de Cloud APM, bajo Mis componentes se visualizan instancias de solo uno de los tipos de componentes de Exchange (Microsoft Exchange Server o Microsoft Exchange Server 2013).

Parámetros de configuración para las propiedades de Exchange Server
En el separador **Propiedades de Exchange Server** de la ventana **Configuración del agente** puede configurar las propiedades de Exchange Server, como nombre de servidor, nombre de dominio y nombre de usuario.

La tabla siguiente contiene descripciones detalladas de los valores de configuración en el separador **Propiedades de Exchange Server**.

Tabla 173. Nombres y descripciones de los valores de configuración en el separador Propiedades de Exchange Server

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos
Nombre de Exchange Server	El nombre del Exchange Server. Durante la instalación de Exchange Server, el nombre del Exchange Server predeterminado es el nombre de host de Windows Server. Si cambia el nombre de Exchange Server predeterminado, debe utilizar el nombre cambiado al configurar el agente de Exchange Server. **Recuerde:** En entornos distribuidos y en clúster, especifique el nombre del servidor de buzón para Exchange Server 2007.	Sí **Importante:** No especifique ningún valor si el agente está instalado en un servidor que tiene un único clúster de copia con más de dos nodos.	Si el nombre de Exchange Server es `popcorn`, escriba `popcorn` en el campo **Nombre de Exchange Server**.
Nombre de dominio de Exchange	El nombre del dominio en el que está instalado el Exchange Server.	Sí	Si Exchange Server está en el dominio `LAB.XYZ.com`, escriba el nombre que precede al primer punto, por ejemplo `LAB`.
Nombre de usuario de Exchange	El nombre del usuario que está configurado para acceder a Exchange Server. **Recuerde:** El usuario debe tener un buzón en el mismo Exchange Server.	Sí	
Contraseña de usuario de Exchange	La contraseña del usuario que está configurado para acceder a Exchange Server.	Sí	
Confirmar contraseña	La misma contraseña que ha especificado para el usuario de Exchange Server.	Sí	

Tabla 173. Nombres y descripciones de los valores de configuración en el separador Propiedades de Exchange Server (continuación)

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos
Nombre de perfil de MAPI de Exchange	Los perfiles de MAPI son los principales valores de configuración necesarios para acceder a Exchange Server. Este campo está inhabilitado si utiliza un Agente de Microsoft Exchange Server de 64 bits para supervisar Exchange Server 2007 o posterior.	No	
Configuración en el clúster	Seleccione este recuadro si desea configurar el Agente de Microsoft Exchange Server en un entorno de clúster.	No aplicable	
Nombre del servidor de clúster	El nombre del servidor de clúster. Este campo está habilitado si marca el recuadro de selección **Configuración en clúster**.	Sí, si está habilitado el campo.	`SCCCluster`
ID de subsistema de Exchange	Nombre del nodo de Cluster Server. Este campo está habilitado si marca el recuadro de selección **Configuración en clúster**.	Sí, si está habilitado el campo.	`nodo1`
Directorio de datos históricos del agente de Exchange	La ubicación en el disco donde se almacenan los datos históricos. Este campo está habilitado si marca el recuadro de selección **Configuración en clúster**.	Sí, si está habilitado el campo.	`c:\history`

Parámetros de configuración de los servicios de Exchange
En el separador **Supervisión de servicios de Exchange** de la ventana **Configuración del agente**, puede seleccionar los servicios de Exchange para conocer el estado de Exchange Server.

La tabla siguiente contiene descripciones detalladas de los valores de configuración de la pestaña **Supervisión de los servicios de Exchange**.

Tabla 174. Nombres y descripciones de los valores de configuración en el separador Supervisión de servicios de Exchange

Nombre de parámetro	Descripción	Campo obligatorio
Servicios de Exchange	Seleccione los servicios de Exchange de la lista disponible de servicios, y pulse la flecha para mover los servicios seleccionados a la lista **Servicios configurados para el estado del servidor** para que el Agente de Microsoft Exchange Server puede supervisarlos. **Recuerde:** La lista de los servicios disponibles cambia según la versión de Exchange Server y los roles que están instalados.	No aplicable
Servicios configurados para el estado del servidor	Los servicios que ya están disponibles en esta lista determinan el estado de Exchange Server. Estos servicios son obligatorios y no se pueden mover de la lista **Servicios configurados para el estado del servidor** a la lista **Servicios de Exchange**. Puede añadir más servicios a la lista **Servicios configurados para el estado del servidor** moviendo los servicios de la lista **Servicios de Exchange**. Puede mover estos servicios adicionales de nuevo a la lista **Servicios de Exchange**.	No aplicable

Parámetros de configuración para la accesibilidad
En el separador **Propiedades de configuración avanzadas** de la ventana **Configuración del agente**, puede configurar los parámetros que están relacionados con la accesibilidad, como dirección de correo electrónico de destino y el intervalo de alcance.

La tabla siguiente contiene descripciones detalladas de los valores de configuración en el separador **Propiedades de configuración avanzadas**.

Tabla 175. Nombres y descripciones de los valores de configuración en el separador Propiedades de configuración avanzadas

Nombre de parámetro	**Descripción**	**Campo obligatorio**
Habilitar supervisión de accesibilidad de buzón	Seleccione este recuadro de selección si desea que el agente capture los datos de métricas de la accesibilidad.	No aplicable
Dirección de correo electrónico de destino	Dirección de correo electrónico para verificar la accesibilidad. Separe varias direcciones de correo electrónico con punto y coma (;). **Restricción:** El número total de caracteres de este campo no debe superar los 1023.	Sí, si está habilitado este campo.
Intervalo de transmisión de correo electrónico (segundos)	El tiempo de espera (en segundos) del agente de Exchange Server entre envío de mensajes de correo electrónico.	Sí, si está habilitado este campo.
Tiempo de espera de transmisión de correo electrónico (segundos)	El intervalo (en segundos) durante el que el agente espera una respuesta al correo electrónico que se ha enviado para probar si el servidor de buzón está accesible.	No
Habilitar supervisión de detalles del buzón	Marque este recuadro de selección para recopilar los datos de las métricas de detalle del buzón.	No aplicable
Hora de inicio de recopilación de detalles del buzón	La hora (en formato de hh:mm:ss) en que se recopilan las métricas de detalle del buzón.	No
Intervalo de recopilación de detalles del buzón (segundos)	El intervalo (en segundos) entre las recopilaciones de métricas de detalles del buzón.	No
Tiempo de recopilación de registros de sucesos (minutos)	Intervalo (en minutos) durante el cual el agente recopila registros de sucesos.	No
Número máximo de sucesos	El recuento máximo hasta el que se recopilan registros de sucesos. La recopilación de registros de sucesos se detiene cuando el número de registros de sucesos recopilados supera el recuento máximo.	No
Intervalo de recopilación (segundos)	El intervalo (en segundos) entre ciclos de agente.	No

Tabla 175. Nombres y descripciones de los valores de configuración en el separador Propiedades de configuración avanzadas (continuación)		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Intervalo de topología de Exchange (segundos)	El intervalo (en segundos) entre las recopilaciones de información detallada de topología.	No
Intervalo de recopilación de seguimiento de mensajes (horas)	El intervalo (en horas) durante el que se recopilan los registros de seguimiento de mensajes. **Restricción:** El valor del intervalo debe estar en el rango 1 - 12. Si especifica un valor de intervalo mayor que 12, el valor se guardará como 12. Si especifica un valor no válido que contiene letras o caracteres especiales, el valor se guardará como 0, lo que indica que la recopilación de seguimiento de mensajes está inhabilitada. Este campo está inhabilitado si se cumple alguna de las condiciones siguientes: • El rol de servidor de buzón o el rol de transporte de concentrador no está instalado en Exchange Server. • La función de seguimiento de mensajes está inhabilitada en Exchange Server.	No

Validación de valores de configuración
Los valores que especifica al configurar el agente se validan. La validación asegura que los valores se han especificado para todos los parámetros obligatorios y que se cumplen ciertas condiciones, como los derechos de administrador local para el usuario.

La tabla siguiente muestra las pruebas de validación que se han realizado en los valores de configuración especificados.

Tabla 176. Pruebas de validación	
Prueba de validación	**Verifica si**
Nombre de Exchange Server	El nombre del servidor de buzón del usuario coincide con el nombre especificado de Exchange Server.
Derechos de Exchange Server	El usuario tiene los derechos de Exchange Server necesarios. En Exchange Server 2007, el usuario debe tener derechos de administrador de destinatarios, y en Exchange Server 2010 o posterior, el usuario debe tener derechos de gestión de destinatarios.
Administración local	El usuario tiene derechos de administrador local.
Inicio de sesión del servicio de agente	El servicio de agente está configurado para ejecutarse con la cuenta de usuario especificada.

Si falla una o más de las pruebas, se genera un mensaje de error. Debe especificar valores para todos los parámetros obligatorios. De lo contrario, no podrá guardar los valores configurados.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para configurar los diferentes valores de los parámetros de configuración del agente.

Acerca de esta tarea
Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

1. Abra el archivo `msex_silent_config.txt` ubicado en *`dir_instalación`*`\samples` y especifique valores para todos los parámetros obligatorios.

   También puede modificar los valores predeterminados de otros parámetros.
2. Ejecute el mandato siguiente:

   `dir_instalación\BIN\msexch-agent.bat config dir_instalación\samples \msex_silent_config.txt`

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Restricción: En el panel de instrumentos de Cloud APM, bajo Mis componentes se visualizan instancias de solo uno de los tipos de componentes de Exchange (Microsoft Exchange Server o Microsoft Exchange Server 2013).

Configuración de variables de entorno locales para el agente

Puede configurar las variables de entorno locales para Agente de Microsoft Exchange Server para habilitar o inhabilitar la regulación de sucesos para sucesos duplicados.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. En la ventana **IBM Performance Management**, desde el menú **Acciones** , pulse **Avanzadas** > **Editar archivo ENV**.
3. En el archivo KEXENV, cambie los valores de las siguientes variables de entorno:

   `EX_EVENT_THROTTLE_ENABLE`
   Esta variable le permite regular sucesos duplicados. El valor predeterminado es `False`. Para permitir que la regulación de sucesos impida el desencadenante de situaciones de sucesos duplicados, establezca el valor de esta variable en True.

   `EX_EVENT_THROTTLE_DURATION`
   Esta variable proporciona la duración (en minutos) para la regulación de sucesos. El valor predeterminado es `0` minutos.

Configuración de la supervisión de Microsoft Hyper-V

Cuando instala Monitoring Agent for Microsoft Hyper-V Server, el agente se configura e inicia automáticamente con los valores de configuración predeterminados. Utilice el archivo de respuestas silencioso para modificar los valores de configuración predeterminados.

Antes de empezar

- Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Microsoft Hyper-V Server.
- Cree un archivo de respuesta que contenga los parámetros de configuración que desea modificar.

- Para ver los datos de sistema virtual en la página de Máquina virtual, asegúrese de instalar el componente de integración y el agente de sistema operativo en cada máquina virtual. Para máquinas virtuales que se ejecutan en el sistema Linux, asegúrese de realizar las tareas siguientes:
  - Actualice el sistema Linux.
  - Instale el paquete `hypervkvpd` o `hyperv-daemons rpm` actualizado en la máquina virtual.

Acerca de esta tarea

Puede configurar el agente si el agente está detenido o en ejecución. El agente permanece en el mismo estado después de la configuración. Por ejemplo, si el agente está en ejecución, permanece en estado de ejecución después de la configuración.

Importante: Para el release 8.1.3 de Performance Management, la ventana de configuración de agente se ha eliminado porque no es necesaria. La ventana de configuración del agente está disponible para 8.1.2, o versiones anteriores de Performance Management.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Procedimiento

Para configurar el agente, realice los pasos siguientes:

1. Abra el archivo `microsoft_hyper-v_server_silent_config.txt` ubicado en *`dir_instalación`*`\samples` y especifique valores para todos los parámetros obligatorios.

   También puede modificar los valores predeterminados de otros parámetros.
2. Abra el indicador de mandatos y especifique el mandato siguiente:

   `dir_instalación\BIN\microsoft_hyper-v_server-agent.bat config dir_instalación\samples\microsoft_hyper-v_server_silent_config.txt`

   El archivo de respuestas contiene los parámetros siguientes:

   - KHV_DIRECTOR_PORT
   - KHV_DIRECTOR_SERVER

   Recuerde: La configuración de agente está organizada en los siguientes grupos:

   Configuración de IBM Systems Director (IBM_DIRECTOR_CONFIGURATION)
   Los elementos de configuración que se definen en este grupo están siempre presentes en la configuración del agente. Este grupo define información que se aplica a todo el agente.

   Número de puerto de IBM Systems Director Server (KHV_DIRECTOR_PORT)
   El número de puerto de IBM Systems Director Server. El valor predeterminado es ninguno.

   Nombre de host de IBM Systems Director Server (KHV_DIRECTOR_SERVER)
   El nombre de host o dirección IP del servidor de IBM Systems Director que está gestionando el entorno. El valor predeterminado es ninguno.
3. Inicie el agente si está en estado detenido.

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Cómo proporcionar una política de seguridad local para ejecutar el agente de supervisión para Microsoft Hyper-V Server en Windows mediante un usuario no administrador

Las políticas de seguridad locales están disponibles para que un usuario no administrador ejecute un Monitoring Agent for Microsoft Hyper-V Server en Windows.

Acerca de esta tarea

Se aplica una combinación de las dos siguientes políticas de seguridad local para que un usuario no administrador ejecute el Agente de Microsoft Hyper-V Server en Windows. Para iniciar o detener, configurar y verificar datos del Agente de Microsoft Hyper-V Server, utilice estas dos políticas.

- Depurar programas
- Iniciar sesión como servicio

Además, los siguientes grupos de atributos necesitan derechos de administrador para obtener datos de un portal de APM:

- Disponibilidad
- Migración
- Clúster de WO Mig de VM
- Migración de almacenamiento de máquina virtual

Siga el procedimiento indicado para otorgar los permisos de seguridad local para un usuario no administrador.

Procedimiento

1. Instale el agente de Microsoft Hyper-V Server como administrador local.
2. Añada el usuario no administrador en el directorio `dir_instalación` y confiérale los permisos siguientes:
   a) Proporcione acceso completo al registro `HKEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring`.
   b) Proporcione acceso de lectura al usuario no administrador al registro `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`.
   c) Proporcione acceso completo al usuario no administrador al directorio `dir_instalación`.
3. Vaya al menú **Inicio** y ejecute el mandato **`secpol.msc`** para abrir las políticas de seguridad locales.
4. Para añadir un usuario no administrador en las políticas, consulte "Cómo otorgar permisos de política de seguridad local" en la página 530.
5. Para añadir un usuario no administrador en el grupo Usuarios administradores de Hyper-V, consulte "Adición de un usuario no administrador al grupo de usuarios administradores de Hyper-V" en la página 532.
6. Para añadir un usuario no administrador en el grupo Usuarios del supervisor de rendimiento, consulte "Adición de un usuario no administrador al grupo de usuarios de Performance Business Monitor" en la página 532.
7. Para modificar el permiso de seguridad de DCOM para un usuario no administrador, consulte "Modificación de permisos de DCOM" en la página 531.
8. Reinicie el Agente de Microsoft Hyper-V Server y verifique los datos del portal de APM.

Cómo otorgar permisos de política de seguridad local

Para iniciar o detener, configurar y verificar datos del Agente de Microsoft Hyper-V Server, tiene que conceder permisos a estas dos políticas de seguridad local: Depurar programas y Iniciar sesión como servicio.

Otorgar el permiso Depurar programas

Acerca de esta tarea

Para otorgar el permiso Depurar programas, complete el siguiente procedimiento.

Procedimiento

1. Pulse **Inicio > Panel de control > Herramientas administrativas > Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.

2. Expanda **Políticas locales** y pulse **Asignación de derechos de usuario**. Se abrirá la lista de políticas.
3. Realice una doble pulsación en la política **Depurar programas**. Se abre la ventana **Propiedades de Depurar programas**.
4. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.
5. En el campo **Especificar los nombres de objeto a seleccionar**, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
6. Pulse **Aplicar** y luego **Aceptar**.

Otorgar el permiso Iniciar sesión como servicio

Acerca de esta tarea

Para otorgar el permiso Iniciar sesión como servicio, complete el procedimiento siguiente.

Procedimiento

1. Pulse **Inicio > Herramientas administrativas > Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.
2. Expanda **Políticas locales** y pulse **Asignación de derechos de usuario**. Se abrirá la lista de políticas.
3. Efectúe una doble pulsación en la política **Iniciar sesión como servicio**. Se abre la ventana **Propiedades de Iniciar sesión como servicio**.
4. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.
5. En el campo **Especificar los nombres de objeto a seleccionar**, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
6. Pulse **Aplicar** y luego **Aceptar**.

Modificación de permisos de DCOM

Tiene que modificar los permisos DCOM para ejecutar el Agente de Microsoft Hyper-V Server con acceso de usuario no administrador.

Acerca de esta tarea

Para modificar los permisos DCOM, verifique que el usuario tenga los permisos correspondientes para iniciar el servidor DCOM. Para modificar permisos, complete el siguiente procedimiento.

Procedimiento

1. Mediante el mandato **Regedit**, vaya al valor de registro `HKCR\Clsid\*clsid value`.

   Nota: cuando se configura el agente con un usuario no administrador, el valor de CLSID se visualiza en el visor de sucesos con el ID de suceso 10016.
2. En el panel Editor del registro, efectúe una doble pulsación en **Valor predeterminado**.
3. En el cuadro de diálogo **Editar serie**, copie la serie de los datos del valor.
4. Pulse **Inicio > Panel de control > Herramientas administrativas > Servicios de componente**.
5. En la ventana **Servicios de componentes**, expanda **Servicios de componentes > Equipos > Mi PC** y efectúe una doble pulsación en **DCOM**.
6. En el panel de configuración de DCOM, localice la serie copiada (nombre de programa), pulse el botón derecho del ratón en el nombre del programa y, a continuación, pulse **Propiedades**.
7. En la ventana **Propiedades**, seleccione la pestaña **Seguridad**.
8. En el cuadro de grupo **Permisos de inicio y activación**, seleccione **Personalizar** y, a continuación, pulse **Editar**. Se abre la ventana **Permisos de inicio y activación**.
9. Pulse **Añadir**, escriba un usuario no administrador en la lista de permisos y pulse **Aceptar**.
10. Marque el recuadro de selección **Permitir** para Inicio local y Activación local y, a continuación, pulse **Aceptar**.

Adición de un usuario no administrador al grupo de usuarios administradores de Hyper-V

Tiene que añadir un usuario no administrador al grupo de usuarios administradores de Hyper-V para obtener datos en el portal de APM.

Acerca de esta tarea

Para añadir un usuario no administrador al grupo de usuarios administradores de Hyper-V, lleve a cabo el siguiente procedimiento.

Procedimiento

1. Pulse **Inicio > Panel de control > Herramientas administrativas > Administración de equipos**. Se abre la ventana **Administración del equipo**.
2. Pulse **Herramientas del sistema > Usuarios y grupos locales > Grupos**. Se abrirá la lista de grupos.
3. Efectúe una doble pulsación en el grupo **Administradores de Hyper-V**. Se abre la ventana **Propiedades de administradores de Hyper-V**.
4. Pulse **Añadir**. Se abre la ventana **Seleccionar usuarios o grupos**.
5. En el campo **Especificar los nombres de objeto a seleccionar**, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
6. Pulse **Aplicar** y luego **Aceptar**.

Adición de un usuario no administrador al grupo de usuarios de Performance Business Monitor

Tiene que añadir un usuario no administrador al grupo de usuarios del supervisor de rendimiento para obtener datos del portal de APM.

Acerca de esta tarea

Para añadir un usuario no administrador al grupo de usuarios de Performance Business Monitor, lleve a cabo el siguiente procedimiento.

Procedimiento

1. Pulse **Inicio > Panel de control > Herramientas administrativas > Administración de equipos**. Se abre la ventana **Administración del equipo**.
2. Pulse **Herramientas del sistema > Usuarios y grupos locales > Grupos**. Se abrirá la lista de grupos.
3. Efectúe una doble pulsación en el grupo **Usuarios del supervisor de rendimiento**. Se abrirá la ventana **Propiedades de usuarios de Performance Business Monitor**.
4. Pulse **Añadir**. Se abre la ventana **Seleccionar usuarios o grupos**.
5. En el campo **Especificar los nombres de objeto a seleccionar**, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
6. Pulse **Aplicar** y luego **Aceptar**.

Configuración de la supervisión de Microsoft IIS

Cuando instala Monitoring Agent for Microsoft Internet Information Services, el agente se configura automáticamente y se inicia con los valores de configuración predeterminados.

Antes de empezar

- Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Microsoft IIS.

- Asegúrese de que el usuario que se conecta a la aplicación o al entorno de Microsoft Internet Information Server tiene privilegios de administrador. Utilice un usuario existente con privilegios de administrador, o cree un nuevo usuario. Asigne privilegios de administrador al nuevo usuario añadiendo el nuevo usuario al grupo Administradores.

  Recuerde: Para configurar Agente de Microsoft IIS, puede utilizar un usuario de dominio o local siempre que el usuario tenga privilegios de administrador.

Acerca de esta tarea

Puede configurar el agente si el agente está detenido o en ejecución. El agente permanece en el mismo estado después de la configuración. Por ejemplo, si el agente está en ejecución, permanece en estado de ejecución después de la configuración.

Para configurar el agente, puede utilizar la ventana de **IBM Performance Management** o el archivo de respuestas silencioso.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Qué hacer a continuación

Después de configurar el agente, puede cambiar la cuenta de usuario del usuario local por el usuario de dominio. Para ver los pasos para cambiar la cuenta de usuario, consulte "Cambio de la cuenta de usuario" en la página 535.

Configuración del agente en sistemas Windows

Puede configurar el Agente de Microsoft IIS en sistemas operativos Windows utilizando la ventana **IBM Performance Management**. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Acerca de esta tarea

Puede configurar el agente si el agente está detenido o en ejecución. El agente permanece en el mismo estado después de la configuración. Por ejemplo, si el agente está en ejecución, permanece en estado de ejecución después de la configuración.

El Agente de Microsoft IIS proporciona valores predeterminados para algunos parámetros. Puede especificar diferentes valores para estos parámetros.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Monitoring Agent for Microsoft Internet Information Services** y luego pulse **Volver a configurar**.
3. En la ventana Monitoring Agent for Microsoft Internet Information Services, realice los pasos siguientes:
   a) En la pestaña **Configuración del registro de errores HTTP**, especifique una ubicación para guardar el archivo de registro, y pulse **Siguiente**.

      Nota: De forma predeterminada, este archivo de registro se guarda en la ubicación siguiente: `C:\WINDOWS\system32\LogFiles\HTTPERR`. El administrador puede cambiar la ubicación del archivo de registro.

   b) En la pestaña **Configuración del registro del sitio**, especifique una ubicación para guardar el archivo de registro, y pulse **Aceptar**.

Nota: De forma predeterminada, este archivo de registro se guarda en la ubicación siguiente: `C:\inetpub\logs\LogFiles`. El administrador puede cambiar la ubicación del archivo de registro.

4. En la ventana **Reinicio de Monitoring Agent for Microsoft IIS**, pulse **Sí**.

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente mediante el archivo de respuestas silencioso

Cuando instala Agente de Microsoft IIS, el agente se configura automáticamente y se inicia con los valores de configuración predeterminados. Utilice el archivo de respuestas silencioso para modificar los valores de configuración predeterminados.

Antes de empezar

Cree un archivo de respuesta que contenga los parámetros de configuración que desea modificar. Si desea modificar los parámetros de configuración predeterminados, edite el archivo de respuestas.

Acerca de esta tarea

Puede configurar el agente si el agente está detenido o en ejecución. El agente permanece en el mismo estado después de la configuración. Por ejemplo, si el agente está en ejecución, permanece en estado de ejecución después de la configuración.

Procedimiento

Para configurar el Agente de Microsoft IIS, complete estos pasos:

1. En la línea de mandatos, cambie la vía de acceso al directorio que contiene el archivo `msiis-agent.bat`.
2. Escriba el mandato siguiente: **`msiis-agent.bat config`** *vía de acceso absoluta al archivo de respuestas*.

   El archivo de respuestas contiene los parámetros siguientes:

   KQ7_SITE_LOG_FILE
   C:\inetpub\logs\LogFiles

   KQ7_HTTP_ERROR_LOG_FILE
   C:\WINDOWS\system32\LogFiles\HTTPERR

   Recuerde: La configuración de agente está organizada en los siguientes grupos:

   Configuración del registro del sitio (SITE_LOG)
   Este grupo contiene los parámetros de configuración que están relacionados con el archivo de registro del sitio (KQ7_SITE_ERROR_LOG_FILE). Un administrador puede especificar una ubicación para guardar el archivo de registro. De forma predeterminada, este archivo de registro se guarda en la ubicación siguiente: `C:\inetpub\logs\LogFiles`

   Configuración de registro de errores de HTTP (HTTP_ERROR_LOG)
   Este grupo contiene los parámetros de configuración que están relacionados con el archivo de registro de errores de HTTP (KQ7_HTTP_ERROR_LOG_FILE). Un administrador puede especificar una ubicación para guardar el archivo de registro. De forma predeterminada, este archivo de registro se guarda en la ubicación siguiente: `C:\WINDOWS\system32\LogFiles\HTTPERR`.
3. Si el agente se encuentra en estado detenido, inicie el agente.

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Cambio de la cuenta de usuario

Después de configurar Agente de Microsoft IIS, puede cambiar la cuenta de usuario del usuario local al usuario de dominio.

Acerca de esta tarea
De forma predeterminada, Agente de Microsoft IIS se ejecuta bajo la cuenta de usuario local.

Procedimiento

1. Ejecute el mandato siguiente para verificar qué ID de usuario se utiliza para iniciar el agente:

   ```
   dir_instalación\InstallITM\KinCinfo.exe -r
   ```
2. Si el agente de supervisión se ha iniciado con un ID de usuario que no pertenece al grupo Administrador, detenga el agente.
3. Abra la ventana **Gestionar servicios de supervisión**.
4. Pulse con el botón derecho en la instancia de agente y, a continuación, pulse **Cambiar inicio**.
5. Especifique el ID de usuario completo como <Dominio\ID de usuario> y, a continuación, especifique la contraseña.
6. Inicie Agente de Microsoft IIS.

Configuración de la supervisión de Skype for Business Server (anteriormente conocido como Microsoft Lync Server)

Cuando instale el Monitoring Agent for Skype for Business Server (anteriormente conocido como MS Lync Server), el agente se hallará en estado no configurado. Para iniciar el agente, tiene que configurarlo.

Antes de empezar

- Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Skype for Business Server.
- Asegúrese de que el usuario que utiliza para ejecutar el Agente de Skype for Business Server, sea un usuario de dominio con privilegios de administrador y que tenga acceso a todos los servidores remotos que aparecen en la lista de topología de Lync o Skype for Business Server. Utilice un usuario de dominio existente con privilegios de administrador, o cree un nuevo usuario de dominio y asignar privilegios de administrador al nuevo usuario de dominio.

Acerca de esta tarea

Puede configurar el agente si el agente está detenido o en ejecución. El agente permanece en el mismo estado después de la configuración. Por ejemplo, si el agente está en ejecución, permanece en estado de ejecución después de la configuración.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Para configurar el agente, puede utilizar la ventana de **IBM Performance Management** o el archivo de respuestas silencioso.

Qué hacer a continuación

Después de configurar el agente, puede cambiar la cuenta de usuario del usuario local por el usuario de dominio. Para ver los pasos para cambiar la cuenta de usuario, consulte "Cambio de la cuenta de usuario" en la página 538.

Permisos y derechos de acceso para un usuario no administrador

Puede ejecutar el agente de supervisión para Agente de Skype for Business Server como un usuario no administrador; sin embargo, algunas funciones serán inaccesibles.

Permisos de registro

Para crear un usuario no administrador, cree un usuario (no administrador) y configure permisos de registro para el usuario nuevo del siguiente modo.

- Acceso completo a KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring
- Acceso completo al directorio CANDLE_HOME

El usuario no administrador debe ser miembro de los Usuarios del supervisor de rendimiento y los Usuarios del registro de rendimiento. Si define estos permisos para un usuario no administrador, se visualizan datos para todos los grupos de atributos basados en Perfmon.

Ver los datos de grupos de atributos recopilados de la base de datos

Si desea ver datos para los grupos de atributos que se recopilan de la base de datos, debe configurar los permisos siguientes para el usuario no administrador.

- La cuenta de usuario no administrador que se utiliza para ejecutar el Agente de Skype for Business Server debe tener el permiso Depurar programa para añadir un depurador a cualquier proceso.

  De forma predeterminada, el permiso Depurar programa sólo se asigna a las cuentas de administrador y sistema local. Para otorgar el permiso Depurar programa, debe completar los pasos siguientes en el servidor Lync o Skype for Business:

  1. Pulse **Inicio > Herramientas administrativas > Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.
  2. Expanda **Políticas locales** y pulse **Asignación de derechos de usuario**. Se abre la lista de derechos de usuario.
  3. Realice una doble pulsación en la política **Depurar programas**. Se abrirá la ventana **Propiedades de Depurar programas**.
  4. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.
  5. En el campo Especificar los nombres de objeto a seleccionar, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
  6. Pulse **Aceptar**.
- Otorgue el permiso Iniciar sesión como servicio

  Para otorgar el permiso Iniciar sesión como servicio, debe completar los pasos siguientes en el servidor Lync o Skype for Business:

  1. Pulse **Inicio > Herramientas administrativas > Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.
  2. Expanda **Políticas locales** y pulse **Asignación de derechos de usuario**. Se abre la lista de derechos de usuario.
  3. Realice una doble pulsación en la política **Iniciar sesión como servicio**. Se abre la ventana **Propiedades de Iniciar sesión como servicio**.
  4. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.

5. En el campo Especificar los nombres de objeto a seleccionar, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
6. Pulse **Aceptar**.

El grupo de atributos Disponibilidad muestra datos para los usuarios que son miembros del grupo de administradores.

Configuración del agente en sistemas Windows

Puede configurar el Agente de Skype for Business Server (anteriormente conocido como agente de MS Lync Server) en sistemas operativos Windows utilizando la ventana **IBM Performance Management**. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Acerca de esta tarea

Puede configurar el agente si el agente está detenido o en ejecución. El agente permanece en el mismo estado después de la configuración. Por ejemplo, si el agente está en ejecución, permanece en estado de ejecución después de la configuración.

El Agente de Skype for Business Server proporciona valores predeterminados para algunos parámetros. Puede especificar diferentes valores para estos parámetros.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Monitoring Agent for Skype for Business Server** y luego pulse **Configurar agente**.
3. En la ventana Monitoring Agent for Skype for Business Server, realice los pasos siguientes:
   a) En la pestaña **Configuración SQL para la topología de Skype for Business**, para conectar con Microsoft Lync Server o Skype for Business Server Central Management Store, especifique los valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.

      Nota: Puede saltarse esta pestaña, ya que Configuración de SQL para topología de Skype for Business no es aplicable para IBM Cloud Application Performance Management.

      Importante: La configuración de transacción sintética es opcional. Si necesita los datos de transacción sintética, especifique los parámetros de configuración en las pestañas **Información de configuración** y **Configuración del planificador**.
   b) En la pestaña **Credenciales de inicio de sesión del administrador**, especifique las credenciales del administrador y a continuación pulse **Siguiente**.
   c) En la pestaña **Información de configuración**, para ejecutar mandatos para las transacciones sintéticas, especifique valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.
   d) En la pestaña **Configuración de planificador**, para planificar las transacciones sintéticas, especifique valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.
   e) En la pestaña **Configuración del servidor SQL para Skype for Business Monitoring Role**, para conectar con Microsoft Lync Server o el rol de supervisión de Skype for Business Server, especifique los valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 539.
4. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Monitoring Agent for Skype for Business Server** y luego pulse **Iniciar**.

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente mediante el archivo de respuestas silencioso

Cuando instale el Agente de Skype for Business Server (anteriormente conocido como agente de MS Lync Server), el agente se hallará en estado desconfigurado. Para iniciar el agente, tiene que configurarlo. El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Antes de empezar

Cree un archivo de respuesta que contenga los parámetros de configuración que desea modificar. Si desea modificar los parámetros de configuración predeterminados, edite el archivo de respuestas.

Acerca de esta tarea

Puede configurar el agente si el agente está detenido o en ejecución. El agente permanece en el mismo estado después de la configuración. Por ejemplo, si el agente está en ejecución, permanece en estado de ejecución después de la configuración.

Procedimiento

Para configurar el Agente de Skype for Business Server, complete estos pasos:

1. Abra el indicador de mandatos.
2. Cambie la vía de acceso al directorio que contiene el archivo `skype_for_business_server-agent.bat`.
3. Escriba el mandato **`skype_for_business_server-agent.bat config`** *vía de acceso absoluta al archivo de respuestas*.

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 539.
4. Inicie el agente si está en estado detenido.

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Cambio de la cuenta de usuario

Después de configurar Agente de Skype for Business Server, puede cambiar la cuenta de usuario del usuario local al usuario de dominio.

Acerca de esta tarea

De forma predeterminada, Agente de Skype for Business Server se ejecuta bajo la cuenta de usuario local. Cuando el agente se ejecuta bajo el usuario de dominio, el agente puede recopilar datos de servidores remotos.

Procedimiento

1. Ejecute el mandato siguiente para verificar qué ID de usuario se utiliza para iniciar el agente:

   `dir_instalación\InstallITM\KinCinfo.exe -r`
2. Si el agente de supervisión se ha iniciado con un ID de usuario que no pertenece al grupo Administrador, detenga el agente.

3. Abra la ventana **Gestionar servicios de supervisión**.
4. Pulse con el botón derecho en la instancia de agente y, a continuación, pulse **Cambiar inicio**.
5. Especifique el ID de usuario completo como <Dominio\ID de usuario> y, a continuación, especifique la contraseña.
6. Inicie Agente de Skype for Business Server.

Parámetros de configuración del agente

Cuando configure el Agente de Skype for Business Server (anteriormente conocido como agente de MS Lync Server), puede cambiar los valores predeterminados de los parámetros de configuración como, por ejemplo, el nombre del servidor de la base de datos, el nombre de la instancia de la base de datos, el nombre de la base de datos y otros parámetros.

La tabla siguiente contiene descripciones de los parámetros de configuración del Agente de Skype for Business Server.

Nota: De todos los campos, el campo Pool FQDN es obligatorio en la siguiente tabla.

Tabla 177. Nombres y descripciones de los parámetros de configuración del agente

Nombre de parámetro	Descripción
Nombre del servidor de bases de datos (por ejemplo, PS6877)	• Pestaña **Configuración SQL para topología Skype for Business**: el nombre del servidor de base de datos donde se ha instalado Lync o Skype for Business Server Central Management Store. • Pestaña **Configuración SQL Server para Skype for Business Monitoring Role**: el nombre del servidor de base de datos donde se ha instalado el rol de supervisión.
Nombre de la instancia de base de datos	• Pestaña **Configuración SQL para topología Skype for Business**: la instancia predeterminada. • Pestaña **Configuración de SQL Server para Skype for Business Monitoring Role**: el nombre de la instancia de base de datos donde se ha instalado el rol de supervisión.
Nombre de base de datos	Nombre de la base de datos.
ID de usuario de base de datos	El ID de usuario de la base de datos. Este usuario debe tener acceso a la instancia de Microsoft SQL Server necesaria. Este usuario es necesario que no sea un usuario de Active Directory.
Contraseña de la base de datos	La contraseña de la base de datos en la que está instalado el rol de supervisión.
Nombre de usuario (Ejemplo: skype \administrator)	ID de usuario del administrador. Este usuario debe ser un usuario de dominio con privilegios de administrador y acceder a todos los servidores remotos que se listan en la topología de Lync o Skype for Business Server. Las credenciales de este usuario también se utilizan en la característica Transacción sintética. Por lo tanto, este usuario debe tener autorización para crear la planificación de Windows en el Planificador de tareas y ejecutar los mandatos de transacción sintética.
Contraseña	Contraseña de inicio de sesión del administrador.
Confirmar contraseña de dominio	Especifique la misma contraseña que ha especificado en el campo Contraseña de dominio.

Tabla 177. Nombres y descripciones de los parámetros de configuración del agente (continuación)

Nombre de parámetro	Descripción
Nombre de dominio completo de agrupación	Nombre de dominio completo (FQDN) de la agrupación Skype para la que se ejecutan mandatos sintéticos.
Ubicación geográfica	Ubicación geográfica del sistema de producción.
Users1 de prueba (por ejemplo, user1@skype.com)	Primer nombre de usuario que se puede utilizar mientras se ejecutan cmdlets de Transacción sintética. El formato para el nombre de usuario es SAMAccountName@domain.com. No proporcione la dirección de Sip.
CTR de User1 de prueba	Contraseña de User1 de prueba.
Confirmar CTR de User1 de prueba	Especifique la misma contraseña que ha especificado en el campo **CTR de User1 de prueba**.
User2 de prueba (por ejemplo, user2@skype.com)	Segundo nombre de usuario que se puede utilizar mientras se ejecutan cmdlets de Transacción sintética. El formato para el nombre de usuario es SAMAccountName@domain.com. No proporcione la dirección de Sip.
CTR de User2 de prueba	Contraseña de User2 de prueba.
Confirmar CTR de User2 de prueba	Especifique la misma contraseña que ha especificado en el campo **CTR de User2 de prueba**.
Utilizar valores de configuración de agente	Mantenga este campo habilitado si desea ejecutar mandatos sintéticos utilizando todos los campos proporcionados en el panel de configuración. Inhabilítelo para utilizar los valores establecidos por New-CsHealthMonitoringConfiguration. Si está inhabilitado, el valor de **Nombre de dominio completo de agrupación** se utilizará como identidad para Get-CsHealthMonitoringConfiguration. Asegúrese de proporcionar credenciales de usuario de prueba válidas para el mandato **Test-CsMcxP2PIM**.
Frecuencia	Frecuencia del programa de utilidad planificada que capta los datos de las transacciones sintéticas. La frecuencia puede tener los valores siguientes: • Diario (DAY_FREQUENCY) • Semanal (WEEK_FREQUENCY) • Mensual (MONTHLY_FREQUENCY)
Hora de recopilación	Parte correspondiente a la hora de la indicación de fecha y hora, en el formato de 24 horas que selecciona para planificar el programa de utilidad.
Minuto de recopilación	Parte correspondiente a los minutos de la indicación de fecha y hora que selecciona para planificar el programa de utilidad.
Fecha de inicio (DD-MM-AAAA)	Hora en que se activa el planificador.
Fecha de finalización (DD-MM-AAAA)	Hora en que se desactiva el planificador.

Configuración de la supervisión de Microsoft .NET

El Monitoring Agent for Microsoft .NET supervisa aplicaciones .NET. El agente se inicia automáticamente después de la instalación para recopilar los datos de supervisión de recursos. Sin embargo, para recopilar datos de diagnósticos y rastreo de transacciones, debe realizar algunas tareas de configuración.

Antes de empezar

Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Microsoft .NET.

Acerca de esta tarea

Una vez instalado el agente, realice las siguientes tareas de configuración para que el agente pueda recopilar los datos de diagnóstico y rastreo de transacciones:

1. Registro del recopilador de datos
   El recopilador de datos es un componente del Agente de Microsoft .NET. Recopila los datos de diagnóstico y rastreo de transacciones y pasa los datos al Agente de Microsoft .NET. Debe registrar el recopilador de datos para recopilar estos datos. Para obtener detalles, consulte "Registro del recopilador de datos" en la página 542.
2. Configuración de la recopilación de datos de diagnóstico y rastreo de transacciones
   Tras registrar el recopilador de datos, habilite la recopilación de datos de diagnóstico y rastreo de transacciones en la Consola de Cloud APM. También puede habilitar la recopilación de datos de diagnóstico mediante el mandato **configdc**. Para obtener detalles, consulte "Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones" en la página 545 y "Habilitación de la recopilación de datos de diagnóstico mediante el mandato configdc" en la página 546.
3. Activación de las actualizaciones de configuración
   Si habilita la recopilación de datos de diagnóstico mediante el mandato **configdc**, debe activar la configuración para que las actualizaciones se guarden en el archivo de configuración. Para obtener más información sobre la activación de los cambios de configuración, consulte "Activación de las actualizaciones de configuración" en la página 548.
4. Ajuste del rendimiento del recopilador de datos
   Puede que sea necesario realizar algunas tareas para ajustar el rendimiento del recopilador de datos. Para obtener detalles, consulte "Ajuste del rendimiento del recopilador de datos" en la página 548.

Coexistencia de agentes

En un entorno de coexistencia de agentes, puede ver datos de rastreo de transacciones desde la Consola de Cloud APM o Tivoli® Enterprise Portal. Para obtener más información acerca de la habilitación de la recopilación de datos para el rastreo de transacciones en el entorno de coexistencia de agentes, consulte "Habilitación del rastreo de transacciones en el entorno de coexistencia de agentes" en la página 547.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Versión de agente. Para acceder a la documentación de los releases anteriores del agente, consulte la tabla siguiente:

Tabla 178. Versiones de agente y documentación

Versión de Agente de Microsoft .NET	Documentación
8.1.3.2	IBM Cloud Application Performance Management
8.1.3 y 8.1.2	IBM Performance Management 8.1.3

El enlace abre un tema del Knowledge Center en local.

Permisos para ejecutar un agente mediante una cuenta local o de dominio

Sólo un usuario local o de dominio miembro del grupo Administradores tiene permisos para ejecutar Agente de Microsoft .NET. Este tema proporciona condiciones que se deben cumplir si el usuario local o de dominio no es un miembro de grupo Administradores.

El usuario debe tener los permisos siguientes en la unidad del sistema y la unidad de instalación del agente

1. Lectura
2. Escritura
3. Ejecución
4. Modificar

El usuario debe tener el permiso siguiente a la clave de registro HKEY_LOCAL_MACHINE

- Lectura

El usuario debe ser miembro de los siguientes grupos en el servidor supervisado

1. Usuarios
2. IIS_IUSRS
3. Usuarios del supervisor de rendimiento
4. Usuarios de registro de rendimiento

Nota: sin embargo, es aconsejable ejecutar el Agente de Microsoft .NET con un usuario local o de dominio que sea miembro del grupo de administradores locales.

Registro del recopilador de datos

Debe registrar el recopilador de datos para recopilar los datos de rastreo de transacciones y diagnóstico. Para recopilar los datos de supervisión de recursos, no se necesita configuración específica.

Acerca de esta tarea

Registre los componentes siguientes del recopilador de datos en función de si el recopilador de datos debe recopilar datos de transacción, de diagnóstico o ambos tipos de datos:

Tabla 179. Componentes del recopilador de datos y sus funciones

Nombre de componente	Supervisa
httpmodule	Transacciones ASP.NET y recopila el tiempo de respuesta de solicitud y el tiempo de CPU
profiler	Transacciones ADO.NET y recopila datos de método, de rastreo de pila y de contexto de solicitud para diagnósticos.
isapi	Transacciones ASP.NET y recopila el tiempo de respuesta de solicitud y el tiempo de CPU
soap	Transacciones de servicio ASMX o WCF y tiempo de respuesta del servicio WCF

Recuerde:

- Utilice `isapi32` para filtrar las aplicaciones de 32-bits en un servidor Microsoft IIS Server de 64-bits.
- Registre todos los componentes para realizar el seguimiento de todas las transacciones y visualizar la topología de transacciones completa.

Procedimiento

1. En el servidor donde está instalado el agente, especifique el mandato siguiente como administrador:

```
cd dir_instalación\qe\bin
configdc.exe registerdc [all|isapi|isapi32|profiler|httpmodule|soap]
```

   Recuerde:

   - Si ejecuta el mandato **configdc.exe registerdc** sin especificar componentes que registrar, sólo se registrará httpmodule.
   - Para registrar todos los componentes, ejecuta el mandato **configdc.exe registerdc all**.
   - Para registrar cualesquiera de los componentes juntos, ejecute este mandato: **configdc.exe registerdc** *nombre_componente nombre_componente*. Por ejemplo, **configdc.exe registerdc** httpmodule profiler
2. Reinicie las aplicaciones .NET.

Qué hacer a continuación
Tras registrar el recopilador de datos, debe habilitar la recopilación de datos para los diagnósticos y el rastreo de transacciones. Para obtener más información acerca de la habilitación de la recopilación de datos, consulte "Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones" en la página 545.

Si desea dejar de supervisar las aplicaciones .NET, anule el registro del recopilador de datos. Repita los pasos indicados utilizando el mandato **configdc.exe unregisterdc** para anular el registro de todos los componentes del recopilador de datos.

Utilización del módulo Tiempo de respuesta de IIS del agente .NET

Desde la versión 8.1.4.0.2 en adelante, el agente .NET incluye el "Módulo Tiempo de respuesta de IIS" que funciona con el agente de tiempo de respuesta con el fin de mostrar datos de transacciones de usuario final para el servidor IIS.

Habilitación del módulo Tiempo de respuesta
Tiene que habilitar el módulo Tiempo de respuesta antes de utilizarlo.

Procedimiento

Complete los pasos siguientes para habilitar el módulo Tiempo de respuesta:

1. Abra el indicador de mandatos en modalidad de Administrador.
2. Para detener IIS, ejecute el mandato siguiente:

   ```
   iisreset /stop
   ```
3. Vaya al directorio `dir_instalación\qe\bin` en el indicador de mandatos.
4. Para registrar el módulo Tiempo de respuesta para IIS, ejecute el mandato siguiente:

   ```
   configdc registerdc rtmodule
   ```
5. Para iniciar IIS, ejecute el mandato siguiente:

   ```
   iisreset /start
   ```

Resultados
El módulo Tiempo de repuesta se ha habilitado.

Configuración del agente de Tiempo de respuesta para que funcione con el módulo Tiempo de respuesta de IIS del agente .NET
Tiene que configurar el agente de Tiempo de respuesta para que funcione con el módulo Tiempo de respuesta de IIS del agente .NET.

Antes de empezar
Instale el agente de Tiempo de respuesta (versión 8.1.4), para obtener más información, consulte Capítulo 6, “Instalación de los agentes”, en la página 125.

Procedimiento

Lleve a cabo los pasos siguientes para configurar el agente de Tiempo de respuesta con el fin de que funcione con el módulo Tiempo de respuesta de IIS del agente .NET:

1. Abra un editor de texto en la modalidad de Administrador.
2. Abra el siguiente archivo en un editor de texto:

   dir_config\TMAITM6_x64*nombre_host*_T5.config

   siendo *dir_config* el directorio de inicio de APM y *nombre_host* es el nombre del servidor.
3. Actualice la propiedad siguiente:

   { KT5DISABLEANALYZER=YES } { KT5ENABLEWEBPLUGIN=YES }
4. Añada la propiedad siguiente en la sección SECTION=analyzerconfig [ ]:

   {KT5WEBPLUGINIPCNAME=KFC1}
5. Reinicie el agente de Tiempo de respuesta.
6. Inicie sesión en la consola de Performance Management para verificar los datos recopilados por el agente en los paneles de instrumentos. Para obtener información acerca de cómo usar la consola de Performance Management, consulte “Inicio de la Consola de Cloud APM” en la página 1009.

Configuración de la inyección JavaScript para el módulo Tiempo de respuesta de IIS
Debe configurar la inyección JavaScript (JS) para que funcione con el módulo TIempo de respuesta de Internet Information Services (IIS)del agente .NET.

Procedimiento

Para configurar la inyección JS para que funcione con el módulo Tiempo de respuesta de IIS del agente .NET, siga estos pasos:

1. Abra un editor de texto en la modalidad de Administrador.
2. Abra el siguiente archivo en un editor de texto:

   <APM_HOME>\qe\config\dotNetDcConfig.properties.inactive
3. Para habilitar la inyección JS para el módulo Tiempo de respuesta, establezca la propiedad **RTModule.JSInjection.Enabled** en **true**.
4. Para inhabilitar la inyección JS para el módulo Tiempo de respuesta, establezca la propiedad **RTModule.JSInjection.Enabled** en **false**.
5. Abra el indicador de mandatos en modalidad de administrador y vaya al directorio <APM_HOME>\qe\bin.
6. Ejecute los mandatos siguientes:
   - configdc activateconfig
   - iisreset

Inhabilitación del módulo Tiempo de respuesta de IIS
Puede inhabilitar el módulo Tiempo de respuesta de IIS cuando no desee ver datos de transacciones de usuarios finales para el servidor ISS.

Procedimiento

Lleve a cabo los pasos siguientes para inhabilitar el módulo de tiempo de respuesta de IIS:

1. Abra el indicador de mandatos en modalidad de Administrador.
2. Para detener IIS, ejecute el mandato siguiente:

```
iisreset /stop
```

3. Vaya al directorio *dir_instalación*\qe\bin en el indicador de mandatos.
4. Para anular el registro del módulo Tiempo de respuesta para IIS, lleve a cabo los pasos siguientes:
   - Para anular el registro del módulo Tiempo de respuesta para IIS, ejecute el mandato siguiente:

     ```
     configdc unregisterdc rtmodule
     ```
   - Para anular registro de todos los componentes del recopilador de datos, incluido el módulo Tiempo de respuesta, ejecute el mandato siguiente:

     ```
     configdc unregisterdc all
     ```
5. Para iniciar IIS, ejecute el mandato siguiente:

   ```
   iisreset /start
   ```

Resultados
El módulo Tiempo de respuesta de IIS se inhabilita.

Limitaciones del módulo Tiempo de respuesta de IIS
A continuación se listan las limitaciones del módulo Tiempo de respuesta de IIS.

- El módulo Tiempo de respuesta de IIS no realiza ningún seguimiento de la información de usuario y el nombre de usuario aparece como "Desconocido".

Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones

En la página **Configuración de agente**, puede habilitar o inhabilitar la recopilación de datos de rastreo de transacciones o diagnóstico.

Antes de empezar
Asegúrese de que ha registrado el recopilador de datos. Para obtener detalles, consulte “Registro del recopilador de datos” en la página 542.

Procedimiento

Complete los pasos siguientes para configurar la recopilación de datos para cada sistema gestionado.

1. Inicie la sesión en la Consola de Cloud APM.
2. En la barra de navegación, pulse **Configuración del sistema** > **Configuración del agente**.
   Se mostrará la página **Configuración del agente**.
3. Pulse la pestaña **MS .NET**.
4. Marque los recuadros de selección de los sistemas gestionados para los que desea configurar la recopilación de datos y lleve a cabo una de las acciones siguientes de la lista **Acciones**.
   - Para habilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Habilitado**. El estado de la columna **Rastreo de transacciones** se actualiza a Habilitado para cada sistema gestionado seleccionado.
   - Para habilitar la recopilación de datos de diagnóstico, seleccione **Establecer modalidad de diagnóstico** y pulse el nivel que desea establecer. El estado de la columna **Modalidad de diagnóstico** se actualiza para mostrar el nivel especificado para cada sistema gestionado seleccionado.
     – Nivel 1: el módulo HTTP recopila los datos de instancia de solicitud y resumen de solicitud.
     – Nivel 2: el módulo HTTP recopila los datos de instancia de solicitud y resumen de solicitud. El perfilador recopila datos de método y datos de rastreo de la pila.
   - Para inhabilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Inhabilitado**. El estado de la columna **Rastreo de transacciones** se actualiza a Inhabilitado para cada sistema gestionado seleccionado.

- Para inhabilitar la recopilación de datos de diagnóstico, pulse **Establecer la modalidad de diagnóstico** > **Inhabilitado**. El estado en la columna **Modalidad de diagnóstico** se actualiza a Inhabilitado para cada sistema gestionado seleccionado.

Resultados
La recopilación de datos se ha configurado para cada sistema gestionado.

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos de diagnóstico y rastreo de transacciones recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Habilitación de la recopilación de datos de diagnóstico mediante el mandato configdc

También puede habilitar o inhabilitar la recopilación de datos de diagnóstico mediante el mandato **configdc**. Este proceso es opcional.

Antes de empezar

- Asegúrese de que ha registrado el recopilador de datos. Para obtener detalles, consulte "Registro del recopilador de datos" en la página 542.
- Asegúrese de que ha completado el proceso de "Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones" en la página 545.
- Asegúrese de que el servidor APM procesa el archivo `qe_custom.properties` en `<APM_Home>\localconfig\qe` y que tiene las propiedades siguientes:
  - transaction_tracking=ENABLED
  - diagnostic_mode=LEVEL2

Procedimiento

1. Ejecute el mandato siguiente:

   ```
   cd dir_instalación\qe\bin configdc deepdivedc -tracelevel nivel_rastreo
   ```

   Donde

   dir_instalación
   El directorio de instalación del Agente de Microsoft .NET.

   nivel_rastreo
   El nivel de rastreo que indica la cantidad de datos de diagnóstico que .NET Data Collector recopila. Especifique uno de los valores siguientes:

   0
   La recopilación de datos de diagnóstico está inhabilitada.

   1
   Se inhabilita la recopilación de datos de diagnóstico. El módulo HTTP recopila los datos de instancia de solicitud y resumen de solicitud.

   2
   Se inhabilita la recopilación de datos de diagnóstico. El módulo HTTP recopila los datos de instancia de solicitud y resumen de solicitud. El perfilador recopila datos de método y datos de rastreo de la pila.

   Consejo: al establecer el nivel de rastreo utilizando el mandato **`configdc.exe deepdivedc -tracelevel`**, se establece el valor del parámetro `bci_dc.diagnose.level` en el archivo `dotNetDcConfig.properties`.
2. Active los cambios de configuración.

Para obtener información sobre la activación de cambios, consulte "Activación de las actualizaciones de configuración" en la página 548.

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos de diagnóstico recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Habilitación del rastreo de transacciones en el entorno de coexistencia de agentes

En un entorno de coexistencia de agentes, puede configurar el recopilador de datos para que recopile y pase los datos de rastreo de transacciones a Tivoli Enterprise Portal, que es un componente de IBM Tivoli Monitoring.

Antes de empezar
Debe instalar el Agente de Microsoft .NET, que se entrega como parte de Cloud APM y debe eliminar o anular el registro del componente .NET Data Collector, que se entrega con ITCAM for Microsoft Applications. Utilice el mandato **`configdc.exe unregisterdc`** para anular el registro de todos los módulos del recopilador de datos.

Procedimiento

Para configurar el recopilador de datos para que recopile y pase los datos de rastreo de transacciones a Tivoli Enterprise Portal, complete los pasos siguientes:

1. Vaya al directorio *dir_instalación*`\localconfig\qe`, donde *dir_instalación* es el directorio de instalación del Agente de Microsoft .NET. La vía de acceso predeterminada es `C:\IBM\APM`.
2. Abra el archivo `qe_default.properties` y establezca el valor del parámetro **`transaction_tracking`** en `ENABLED`.
3. Guarde y cierre el archivo `qe_default.properties`.
4. Vaya al directorio *dir_instalación*`\qe\config`.
5. Abra el archivo `dotNetDcConfig.properties.inactive` en un editor de texto.
6. Establezca los parámetros **`TTDC.enabled`** y **`TTAS.enabled`** de esta manera:

```
TTDC.enabled=true
TTAS.enabled=true
```

7. Para configurar la conexión con el recopilador de transacciones, establezca los valores de los parámetros **`TTAS.Host`** y **`TTAS.Port`** en la dirección IP y número de puerto del recopilador de transacciones.
8. Ejecute el mandato siguiente para activar los cambios:

```
dir_instalación\qe\bin\configdc.exe activateconfig
```

9. Reinicie la aplicación .NET para que los cambios entren en vigor.

Resultados
Ahora, los datos de rastreo de transacciones se pueden recopilar y visualizar en Tivoli Enterprise Portal.

Qué hacer a continuación

Para inhabilitar el rastreo de transacciones para un .NET Data Collector, repita el procedimiento y utilice los valores de configuración siguientes:

- En el archivo `qe_default.properties`, establezca `transaction_tracking=DISABLED`.
- En el archivo `dotNetDcConfig.properties.inactive`, establezca `TTDC.enabled=false` y `TTAS.enabled=false`.

Activación de las actualizaciones de configuración

Debe activar las actualizaciones realizadas en los valores de configuración mediante el mandato `configdc`. La activación garantiza que las actualizaciones se guardan en el archivo `dotNetConfig.properties`.

Acerca de esta tarea

Al actualizar los valores de configuración mediante el mandato **`configdc`**, los valores de parámetro se actualizan en el archivo `dotNetConfig.properties`. Sin embargo, si este archivo está en uso y no puede modificarse, las actualizaciones de los valores de configuración se guardarán en el archivo `dotNetDcConfig.properties.inactive`. Debe activar la configuración para que las actualizaciones se guarden en el archivo `dotNetConfig.properties`.

Procedimiento

1. Vaya a la vía de acceso siguiente:
   `dir_instalación``\qe\bin`
   Donde *dir_instalación* es el directorio de instalación del Agente de Microsoft .NET.
2. Ejecute el mandato siguiente:
   `configdc activateConfig`

Qué hacer a continuación

Si se supervisan las transacciones de Internet Information Services (IIS) y se actualiza la configuración del recopilador de datos, reinicie IIS para activar la configuración.

Si se supervisan los servicios web ASMX o WCF y la configuración del recopilador de datos se actualiza, reinicie el proceso que aloja el servicio web.

Ajuste del rendimiento del recopilador de datos

Al configurar el recopilador de datos para recopilar los datos de rastreo de transacciones y diagnóstico, el rendimiento del recopilador de datos resulta afectado. Para mejorar el rendimiento, puede realizar algunas tareas de ajuste del rendimiento.

Puede que sea necesario realizar las tareas siguientes para mejorar el rendimiento del recopilador de datos:

- Filtrar las interfaces ADO.NET que se desea supervisar.
- Muestrear los datos de diagnóstico y rastreo de transacciones.
- Configurar el registro de rastreo.

Especificación de interfaces ADO.NET para la supervisión

Puede especificar las interfaces de cliente ADO.NET que desea habilitar para el rastreo de transacciones.

Antes de empezar

Si desea ver las interfaces ADO.NET admitidas por el .NET Data Collector, consulte Functions of namespaces supported by the data collector (Funciones de espacios de nombres que el recopilador de datos admite).

Para ver los valores de configuración del .NET Data Collector, consulte el archivo `dotNetDcConfig.properties` en el directorio *`dir_instalación`*`\qe\config`, donde *dir_instalación* es el directorio de instalación del Agente de Microsoft .NET.

Acerca de esta tarea

De forma predeterminada, todas las interfaces ADO.NET admitidas están habilitadas para el rastreo de transacciones durante la instalación del agente. Para especificar las interfaces que el recopilador de datos debe supervisar, habilite o inhabilite la supervisión para interfaces específicas.

Si se inhabilita la supervisión de una interfaz, los valores de cualquier filtro de dominio de aplicación asociado permanecen en el archivo de configuración del recopilador de datos. El filtro se mantiene cuando se vuelve a habilitar la interfaz.

Procedimiento

- Para habilitar la supervisión de una interfaz ADO.NET, siga estos pasos:
  a) En el directorio *dir_instalación*\qe\bin, ejecute el mandato siguiente:

```
configdc enableMonitor all | adsi | db2 | ldap | odbc | oledb | oracle | sql
| http | web
[-appdomain lista de filtros de dominio de aplicación]
```

  b) Active los cambios de configuración.

  Para obtener información sobre la activación de cambios, consulte "Activación de las actualizaciones de configuración" en la página 548.
- Para inhabilitar la supervisión de una interfaz ADO.NET, siga estos pasos:
  a) En el directorio *dir_instalación*\qe\bin, ejecute el mandato siguiente:

```
configdc disableMonitor all | adsi | db2 | ldap | odbc | oledb | oracle | sql
| http | web
```

  b) Active los cambios de configuración.

  Para obtener información sobre la activación de cambios, consulte "Activación de las actualizaciones de configuración" en la página 548.

Rastreo de transacciones de muestreo y datos de diagnóstico

Si el rendimiento del sistema resulta afectado por el rastreo de transacciones o la recopilación de datos de diagnóstico, puede habilitar el muestreo de los datos recopilados para mejorar el rendimiento.

Acerca de esta tarea

Cuando el rendimiento del sistema sufre debido al rastreo de transacciones y la recopilación de datos de diagnóstico, puede configurar el recopilador de datos para que periódicamente recopile datos mediante muestreo. Cuando el muestreo está habilitado, el recopilador de datos no recopila los datos para cada solicitud, sino en intervalos de varias solicitudes. Puede cambiar tasa de muestreo dinámicamente de acuerdo con el uso de CPU del proceso DotNetProfilerService.

PRECAUCIÓN: El muestreo puede ahorrar recursos del sistema, pero es posible que los datos de muestreo no sean eficientes para los problemas de diagnóstico. Después de que se habilita el muestreo de datos, es posible que se interrumpa o se pierda la topología de rastreo de transacciones. Por tanto, habilite el muestreo de datos solo cuando el rendimiento se vea seriamente afectado.

Procedimiento

Para habilitar el muestreo en el rastreo de transacciones y la recopilación de datos de diagnóstico, realice los pasos siguientes:

1. Vaya al directorio siguiente:
   dir_instalación\qe\config
   Donde *dir_instalación* es el directorio de instalación del Agente de Microsoft .NET.
2. En un editor de texto, abra el archivo `dotNetDcConfig.properties.inactive`.
3. Establezca los parámetros siguientes en el archivo:

   bci_dc.sampling.Enabled
   especifica si el recopilador de datos recopila periódicamente los datos de diagnóstico y de rastreo de transacciones. Los valores válidos son `true` y `false`.

bci_dc.sampling.base
Especifica la base del muestreo de datos. Un valor válido es un número positivo. Por ejemplo, si establece el valor del parámetro **bci_dc.sampling.base** en 10, el recopilador de datos recopila el rastreo de transacciones y los datos de diagnóstico cada 10 solicitudes. La tasa de muestreo es 1 de 10 solicitudes. El recopilador de datos recopila los datos para la 1ª, 11ª, 21ª, 31ª y otras solicitudes.

bci_dc.dynamic.sampling
Especifica si la tasa de muestreo es constante o dinámica. Los valores válidos son on y off. Cuando establece el valor del parámetro **bci_dc.dynamic.sampling** en on, la tasa de muestreo se ajusta dinámicamente de acuerdo con el valor del parámetro **bci_dc.dynamic.max_cpu_usage**.

bci_dc.dynamic.max_cpu_usage
Especifica el umbral de uso de CPU para el proceso DotNetProfilerService. Si el uso de CPU del proceso DotNetProfilerService es superior al 110 % del valor especificado, disminuye la tasa de muestreo. Si el uso de CPU es inferior al 90 % del valor especificado, aumenta la tasa de muestreo. Un valor válido debe estar en el rango 1 - 100.

4. Guarde y cierre el archivo `dotNetDcConfig.properties.inactive`.
5. Ejecute el mandato siguiente para activar los cambios:

```
dir_instalación\qe\bin\configdc.exe activateconfig
```

6. Reinicie la aplicación .NET para que los cambios entren en vigor.

Habilitación del registro de rastreo para el recopilador de datos

Puede habilitar la generación de registros de rastreo para el recopilador de datos. Puede utilizar estos registros de rastreo para resolver los problemas que pueden producirse en la recopilación de datos de diagnóstico y rastreo de transacciones.

Acerca de esta tarea

Para recopilar registros de transacciones ASP.NET, transacciones ADO.NET y datos de diagnóstico, habilite registros de rastreo para los componentes httpmodule, perfilador e isapi del recopilador de datos. Para recopilar registros de transacciones ASMX y WCF, habilite registros de rastreo para el componente soap del recopilador de datos.

Importante: es posible que el rendimiento del recopilador de datos resulte afectado cuando el registro de rastreo esté habilitado. Por tanto, inhabilite el registro de rastreo una vez recopilados los registros de rastreo necesarios.

Procedimiento

1. En el servidor donde está instalado el agente, vaya a la siguiente vía de acceso:
   dir_instalación\qe\bin
   Donde *dir_instalación* es el directorio de instalación del Agente de Microsoft .NET.
2. Complete uno de los procedimientos siguientes o ambos, en función de los registros de rastreo que desee habilitar:
   - Para habilitar los registros de rastreo para httpmodule, perfilador, componente soap y módulo Tiempo de respuesta, complete los pasos siguientes:
     a. Ejecute el mandato siguiente:
        configdc logging -tracing on
     b. Reinicie las aplicaciones IIS y .NET.
   - Para habilitar los registros de rastreo para el motor BCI, complete los pasos siguientes:
     a. Navegue hasta la vía de acceso siguiente:
        <APM_HOME>\qe\config
     b. En un editor de texto, abra el archivo `dotNetDcConfig.properties.inactive`.

c. Para la propiedad **bci_dc.trace.logging**, especifique el valor como on.

d. Ejecute el mandato siguiente:
configdc activateconfig

e. Reinicie IIS.

Qué hacer a continuación
Para inhabilitar los registros de rastreo, haga lo siguiente:

- Para inhabilitar los registros de rastreo para httpmodule, perfilador, componentes soap y módulo Tiempo de respuesta:
  - Ejecute el mandato siguiente:
    `configdc logging -tracing off`
  - Reinicie las aplicaciones IIS y .NET.
- Para inhabilitar los registros de rastreo para el motor BCI:
  - Vaya a la vía de acceso siguiente:
    `<APM_HOME>\qe\config`
  - En un editor de texto, abra el archivo `dotNetDcConfig.properties.inactive`.
  - Para la propiedad **bci_dc.trace.logging**, especifique el valor como `off`.
  - Ejecute el mandato siguiente:
    configdc activateconfig
  - Reinicie las aplicaciones IIS y .NET.

Configuración de la supervisión de Microsoft Office 365

Debe configurar el Agente de Microsoft Office 365 para supervisar la disponibilidad y el rendimiento de las suscripciones a Microsoft Office 365 de la organización.

Antes de empezar

- Revise los requisitos previos de hardware y software.
- Para recopilar datos para usuarios de Office 365, los módulos siguientes deben instalarse en el cliente Windows donde se ha instalado el agente:
  - PowerShell 3.0 o posterior
  - Microsoft Online Services Sign-In Assistant PowerShell
  - SharePoint Online Management Shell
  - DotNetFrameworkVersion 4.5.2 o posterior

  El usuario que configura el agente debe tener privilegios administrativos junto con privilegios para habilitar la política de ejecución remota de PowerShell.
- Para supervisar transacciones sintéticas de Skype, realice las tareas siguientes:
  - Instale el cliente Skype 2013 en el cliente Windows donde el usuario desea realizar transacciones sintéticas para Skype.
  - Establezca el dispositivo de vídeo predeterminado para Lync y Skype como un filtro de audio y vídeo virtual.
- Asegúrese de que el usuario que inicia Microsoft Office 365 tiene privilegios de administrador. Utilice un usuario existente con privilegios de administrador, o cree un nuevo usuario. Asigne privilegios de administrador al nuevo usuario añadiendo el nuevo usuario al grupo Administradores.

Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Microsoft Office 365.

Acerca de esta tarea

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Agente de Microsoft Office 365. Para acceder a la documentación para V1.0.0, consulte el Knowledge Center de IBM Cloud Application Performance Management.

Puede iniciar el Agente de Microsoft Office 365 después de que se ha instalado el agente. Sin embargo, es necesaria la configuración manual para ver los datos de todos los atributos de agente.

Para configurar el agente, puede utilizar la ventana de IBM Cloud Application Performance Management o el archivo de respuestas silencioso.

Verificación de la accesibilidad de los usuarios configurados

Para verificar la accesibilidad, el Agente de Microsoft Office 365 envía un mensaje de correo electrónico a los usuarios configurados y mide la cantidad de tiempo que se tarda en recibir una respuesta automática. Antes de iniciar el agente, debe configurar todos los usuarios, que se configuran en el valor de accesibilidad del buzón del agente de Office 365, para que respondan automáticamente a los mensajes de correo electrónico.

Antes de empezar

Antes de configurar los usuarios de Exchange Online para la accesibilidad, asegúrese de que se han completado las tareas siguientes:

- Se ha creado un buzón para cada usuario en el Exchange Online que desea supervisar.
- El usuario que ha creado para el agente es un usuario global de Office 365.

Procedimiento

Complete los pasos siguientes para cada cuenta de usuario de Exchange Online para la que desee verificar la accesibilidad:

1. Inicie sesión en Microsoft Outlook especificando las credenciales del usuario que ha creado.
2. Pulse en **Herramientas > Reglas y alertas > Nueva regla**.
3. En la ventana **Asistente para reglas**, bajo **Iniciar desde una regla en blanco**, pulse **Aplicar regla a los mensajes que reciba** y pulse **Siguiente**.
4. Seleccione las opciones siguientes:
   - **De personas o grupo público**
   - **Con cierto texto en el asunto**
5. En el **Paso 2** de la ventana, pulse en **personas o grupo público**.
6. En la ventana **Dirección de regla**, seleccione el usuario (administrador global) del que se van a recibir los mensajes y pulse **Siguiente**.
7. En el **Paso 2** de la ventana, pulse en **cierto texto**.
8. En el campo **Especificar las palabras o frases que desee buscar en el asunto o cuerpo del mensaje**, escriba `Probar accesibilidad`.
9. Pulse **Añadir**.
10. Pulse **Aceptar** y, a continuación, pulse **Siguiente**.
11. Seleccione **disponer de respuesta del servidor mediante un mensaje determinado** y pulse en **un mensaje determinado**.
12. En el editor de mensajes de correo electrónico, escriba el texto siguiente en el campo de asunto del mensaje:

    `Probar accesibilidad`.
13. En la lista **A**, añada el administrador global.
14. Cierre el editor de mensajes de correo electrónico y pulse **Sí** para guardar estos cambios.
15. Pulse **Finalizar**.

16. Pulse **Aplicar** y a continuación pulse **Aceptar**.

Qué hacer a continuación
Configure el Agente de Microsoft Office 365.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente en sistemas Windows

Puede configurar el Agente de Microsoft Office 365 en sistemas operativos Windows utilizando la ventana de IBM Cloud Application Performance Management. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Acerca de esta tarea
Puede configurar el agente si el agente está detenido o en ejecución. El agente permanece en el mismo estado después de la configuración. Por ejemplo, si el agente está en ejecución, permanece en estado de ejecución después de la configuración.

El Agente de Microsoft Office 365 proporciona valores predeterminados para algunos parámetros. Puede especificar diferentes valores para estos parámetros.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en **Monitoring Agent for Microsoft Office 365** y luego pulse **Configurar agente**.
3. En la ventana **Monitoring Agent for Microsoft Office 365**, siga estos pasos:
   a) En la pestaña **Detalles de suscripción a Office365**, especifique el nombre de usuario y la contraseña del administrador global de Office 365 y pulse **Siguiente**.
   b) En la pestaña **Transacción sintética**, especifique la lista de direcciones de correo electrónico delimitadas por signos de punto y coma en el campo **Direcciones de correo electrónico de accesibilidad**.
   c) Para habilitar la recopilación de datos de las métricas de QoS de Sype, marque el recuadro de selección **Skype QoS** y pulse **Siguiente**.
   d) En la pestaña **Supervisión de uso de buzón y OneDrive**, seleccione la duración del intervalo de recopilación en horas en la lista **Intervalo de recopilación** y pulse **Siguiente**.
4. En la ventana **Monitoring Agent for Microsoft Office 365**, pulse **Sí**.

Qué hacer a continuación

- Configure los programas de utilidad de transacción sintética de Skype para supervisar las transacciones sintéticas QoS de Skype. Para obtener más información sobre la supervisión de la QoS de Skype, consulte “Supervisión de la QoS de Skype” en la página 555.
- Cambie la cuenta de usuario del usuario local por el usuario de dominio. Para obtener detalles, consulte “Cambio de la cuenta de usuario” en la página 554.
- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte “Inicio de la Consola de Cloud APM” en la página 1009.
- Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente mediante el archivo de respuestas silencioso

Al instalar el Agente de Microsoft Office 365, el agente debe configurarse e iniciarse manualmente después de proporcionar los valores de configuración. Utilice el archivo de respuestas silencioso para configurar los valores personalizados.

Antes de empezar

Edite el archivo de respuestas para modificar los siguientes valores de configuración predeterminados:

KMO_USER_NAME
El nombre de usuario del administrador global de Office 365

KMO_PASSWORD
La contraseña del administrador global de Office 365.

KMO_MAIL_ADDRESSES1
Lista de direcciones de correo electrónico para verificar la accesibilidad del buzón. La lista de direcciones de correo electrónico deben estar delimitada mediante signos de punto y coma.

KMO_SKYPE
Este parámetro se utiliza para habilitar la recopilación de las transacciones sintéticas de QoS de Skype.

KMO_DATA_COLLECTION_DURATION
Intervalo (en horas) durante el cual el agente espera antes de captar los datos de uso de OneDrive y buzón.

El archivo de respuestas está disponible en la ubicación siguiente:
`<CANDLEHOME>\samples`

Acerca de esta tarea
Puede configurar el agente si el agente está detenido o en ejecución. El agente permanece en el mismo estado después de la configuración. Por ejemplo, si el agente está en ejecución, permanece en estado de ejecución después de la configuración.

Procedimiento

Para configurar el Agente de Microsoft Office 365, complete estos pasos:

1. En el indicador de mandatos, cambie la vía de acceso al directorio que contiene el archivo `microsoft_office365-agent.bat`.
2. Escriba el mandato siguiente: `microsoft_office365-agent.bat` *vía de acceso absoluta al archivo de respuestas*.

   El archivo de respuestas contiene los parámetros siguientes:
3. Si el agente se encuentra en estado detenido, inicie el agente.

Qué hacer a continuación

- Configure los programas de utilidad de transacción sintética de Skype para supervisar las transacciones sintéticas QoS de Skype. Para obtener más información sobre la supervisión de la QoS de Skype, consulte "Supervisión de la QoS de Skype" en la página 555.
- Cambie la cuenta de usuario del usuario local por el usuario de dominio. Para obtener detalles, consulte "Cambio de la cuenta de usuario" en la página 554.
- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.
- Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Cambio de la cuenta de usuario

Después de configurar el Agente de Microsoft Office 365, cambie la cuenta de usuario del usuario local al usuario de dominio.

Acerca de esta tarea
De forma predeterminada, Agente de Microsoft Office 365 se ejecuta bajo la cuenta de usuario local.

Procedimiento

1. Ejecute el mandato siguiente para verificar qué ID de usuario se utiliza para iniciar el agente:

   dir_instalación\InstallITM\KinCinfo.exe -r
2. Si el agente de supervisión se ha iniciado con un ID de usuario que no pertenece al grupo Administrador, detenga el agente.
3. Abra la ventana **Gestionar servicios de supervisión**.
4. En la ventana **Gestionar servicios de supervisión**, pulse la instancia de agente con el botón derecho del ratón y pulse **Cambiar inicio**.
5. Especifique el ID de usuario completo como <Dominio\ID de usuario> y, a continuación, especifique la contraseña.
6. Inicie Agente de Microsoft Office 365.

Supervisión de la QoS de Skype

Para supervisar la QoS de Skype, el usuario debe configurar los programas de utilidad de transacción sintética de Skype, `kmoskypecaller.exe` y `Kmoskypereceiver.exe`, en el cliente Windows donde está instalado el agente o un entorno distribuido donde esté configurado el cliente de Skype for Business.

Antes de empezar

Para realizar transacciones sintéticas, debe actualizar el nombre del emisor y del receptor de Skype en el archivo `<CANDLEHOME>\tmaitm6_x64\kmoskypecallerlist.properties` en el formato siguiente:
`emisor skype = receptor skype`
Por ejemplo, john@xyz.com = alan@xyz.com
Puede añadir varios receptores de llamadas de Skype para un único emisor de Skype en el formato siguiente:
`emisor skype = lista de receptores skype`
Por ejemplo, john@xyz.com = alam@xyz.com;bill@xyz.com;chuk@xyz.com

Recuerde: si no desea realizar transacciones sintéticas pero desea supervisar la QoS de Skype para usuarios en tiempo real, no es necesario actualizar el archivo `<CANDLEHOME>\TMAITM6_x64\kmoskypecallerlist.properties`.

Acerca de esta tarea

Una vez configurado e iniciado el Agente de Microsoft Office 365, se crearán los siguientes archivos y carpetas en `<CANDLEHOME>\TMAITM6_x64\`:

- `kmoskypecaller.properties`
- `kmoskypecallerlist.properties`
- `KMOSynthTransSkype.zip`
- `KMOSkypeTransReceiver.zip`

Además, el archivo `kmoskypecaller.properties` se actualiza con la dirección IP y el puerto del servidor que se utilizan para la comunicación entre el agente y el programa de utilidad kmoskypecaller.

Procedimiento

Para configurar el emisor y los receptores de Skype e iniciar las transacciones sintéticas, como por ejemplo mensajería instantánea, llamadas de audio y vídeo y sesiones de compartimiento de aplicaciones, siga estos pasos:

1. Inicie el agente de Office 365.
2. Copie el archivo `KMOSynthTransSkype.zip` del cliente de agente al cliente de Windows desde donde se va iniciar la llamada de Skype.
3. Extraiga el archivo `KMOSynthTransSkype.zip`.

4. Copie el archivo `kmoskypecaller.properties` del cliente de agente a la carpeta `KMOSynthTransSkype` extraída en el cliente Windows desde el que se va a iniciar la llamada de Skype.
5. Copie el archivo `KMOSkypeTransReceiver.zip` del cliente de agente a todos los clientes Windows en los que se van a recibir las llamadas de Skype.
6. Extraiga el archivo `KMOSkypeTransReceiver.zip` en todos los clientes Windows donde deben recibirse las llamadas de Skype, y ejecute `KMOSkypeTransReceiver.exe` para empezar a recibir mensajes.
7. Para iniciar las transacciones sintéticas, ejecute el archivo `KMOSynthTransSkype.exe`, que está disponible en la carpeta `KMOSynthTransSkype` extraída en el cliente Windows. El agente de Office 365 empezará a recibir los datos de supervisión de Skype del cliente que efectúa la llamada.

Resultados
El agente inicia la supervisión de la QoS de Skype.

Configuración de las variables del entorno local

Puede configurar variables de entorno local para cambiar el comportamiento del Agente de Microsoft Office 365.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, en el menú **Acciones**, pulse **Avanzada > Editar archivo ENV**.
3. En el archivo de variables de entorno, especifique los valores para las variables de entorno.

   Para obtener información sobre las variables de entorno que puede configurar, consulte "Variables de entorno local" en la página 556.

Variables de entorno local
Puede cambiar el comportamiento del Agente de Microsoft Office 365 configurando las variables de entorno local.

Variables para definir el método de recopilación de datos para el agente

Para establecer el método para la recopilación de datos del agente, utilice las siguientes variables de entorno:

- **CDP_DP_INITIAL_COLLECTION_DELAY**: utilice esta variable para establecer el intervalo de tiempo (en segundos) tras el cuál la agrupación de hebras empieza la recopilación de datos.
- **KMO_MAILBOX_REACHABILITY_INTERVAL**: utilice esta variable para establecer el intervalo de recopilación de datos (en minutos) para el grupo de atributos de accesibilidad de buzón.
- **KMO_SKYPE_REPORT_INTERVAL**: utilice esta variable para establecer el intervalo de recopilación de datos (en horas) para la característica de estadísticas de uso de Skype for Business.
- **KMO_SERVICE_API_INTERVAL**: utilice esta variable para establecer el intervalo de recopilación de datos (en minutos) para la característica de estado de servicio de Office 365.
- **KMO_NETWORK_CONNECTION_INTERVAL**: utilice esta variable para establecer el intervalo de recopilación de datos (en minutos) para la característica de conectividad de internet.
- **KMO_NETWORK_PERFORMANCE_INTERVAL**: utilice esta variable para establecer el intervalo de recopilación de datos (en minutos) para la característica de rendimiento de red de servicios de Office 365.
- **KMO_SITE_CONNECTION_INTERVAL**: utilice esta variable para establecer el intervalo de recopilación de datos (en minutos) para la característica de conectividad de Office 365.
- **KMO_SPSITE_COLLECTION_INTERVAL**: utilice esta variable para establecer el intervalo de recopilación de datos (en minutos) para la característica de detalles de SharePoint Sites.

- **KMO_UASGE_STATS_INTERVAL**: utilice esta variable para establecer el intervalo de recopilación de datos (en horas) para la característica de estadísticas de usuario y uso de Office 365 Services.
- **KMO_TENANT_INTERVAL**: utilice esta variable para establecer el intervalo de recopilación de datos (en minutos) para la característica de detalles de arrendatario de Office 365.
- **KMO_ONEDRIVE_CONNECTIVITY_INTERVAL**: utilice esta variable para establecer el intervalo de recopilación de datos (en minutos) para la característica de conectividad de Office 365 OneDrive.
- **KMO_TENANT_DOMAIN**: utilice esta variable para establecer el nombre de dominio del arrendatario.

Configuración de la supervisión de Microsoft SharePoint Server

Cuando instala Monitoring Agent for Microsoft SharePoint Server, el agente se configura e inicia automáticamente con los valores de configuración predeterminados. Utilice el archivo de respuestas silencioso para modificar los valores de configuración predeterminados.

Antes de empezar

Asegúrese de que completa las tareas siguientes:

- Asegúrese de que el usuario que se conecta al entorno o a la aplicación de Microsoft SharePoint Server tiene privilegios de administrador. Utilice un usuario existente con privilegios de administrador, o cree un nuevo usuario. Asigne privilegios de administrador al nuevo usuario añadiendo el nuevo usuario al grupo Administradores.

  Recuerde: Para configurar Agente de Microsoft SharePoint Server, puede utilizar un usuario de dominio o local siempre que el usuario tenga privilegios de administrador.
- Edite el archivo de respuestas y modifique los parámetros de configuración predeterminados.

  El archivo de respuestas contiene los parámetros siguientes:

  KQP_DB_User
  El ID de usuario de la base de datos.

  KQP_DB_Password
  La contraseña de la base de datos.

Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Microsoft SharePoint Server.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Versión de agente. Para acceder a la documentación de los releases anteriores del agente, consulte la tabla siguiente:

Tabla 180. Versiones de agente y documentación

Versión del Agente de Microsoft SharePoint Server	Documentación
06.31.09.00, 06.31.10.00	IBM Cloud Application Performance Management
06.31.09.00	IBM Performance Management 8.1.3 **Nota:** El enlace abre un tema de Knowledge Center en local.
06.31.07.00	IBM Performance Management 8.1.2 **Nota:** El enlace abre un tema de Knowledge Center en local.

Procedimiento

Para configurar el Agente de Microsoft SharePoint Server, complete estos pasos:

1. Abra el indicador de mandatos.
2. Cambie la vía de acceso al directorio que contiene el archivo `ms_sharepoint_server-agent.bat`.
3. Escriba el mandato siguiente: **`ms_sharepoint_server-agent.bat config`** *vía de acceso absoluta al archivo de respuestas*.
4. Si el agente se encuentra en estado detenido, inicie el agente.

Qué hacer a continuación

Después de configurar el agente, puede cambiar la cuenta de usuario del usuario local por el usuario de dominio. Para ver los pasos para cambiar la cuenta de usuario, consulte "Cambio de la cuenta de usuario" en la página 558.

Cambio de la cuenta de usuario

Después de configurar Agente de Microsoft SharePoint Server, puede cambiar la cuenta de usuario del usuario local al usuario de dominio.

Acerca de esta tarea

Con el usuario de dominio, el agente puede supervisar todos los componentes de Agente de Microsoft SharePoint Server.

Procedimiento

Para cambiar la cuenta de usuario, realice los pasos siguientes:

1. Ejecute el mandato siguiente para verificar qué ID de usuario se utiliza para iniciar el agente.

   `dir_instalación\InstallITM\KinCinfo.exe -r`
2. Si el agente de supervisión se ha iniciado con un ID de usuario que no pertenece al grupo Administrador, detenga el agente.
3. Abra la ventana **Gestionar servicios de supervisión**.
4. Pulse con el botón derecho en la instancia de agente y, a continuación, pulse **Cambiar inicio**.
5. Especifique el ID de usuario totalmente calificado como `<Dominio\ID de usuario>` y, a continuación, especifique la contraseña.
6. Inicie el agente de supervisión.

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Ejecución de Monitoring Agent for Microsoft SharePoint Server por parte de un usuario no administrador

Hay políticas de seguridad local disponibles para que un usuario no administrador ejecute un Monitoring Agent for Microsoft SharePoint Server.

Acerca de esta tarea

Se aplica una combinación de las dos siguientes políticas de seguridad local para que un usuario no administrador ejecute el Agente de Microsoft SharePoint Server.

1. Depurar programas.
2. Iniciar sesión como servicio.

Siga el procedimiento indicado para otorgar los permisos de seguridad local para un usuario no administrador.

Procedimiento

1. Vaya a TEMA y cambie el inicio del Agente de Microsoft SharePoint Server con usuario no administrador.
2. Añada el usuario no administrador bajo el directorio HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office Server de clave de registro y otórguele acceso de lectura.
3. Añada el usuario no administrador bajo la clave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions y otórguele acceso de lectura sobre ella.
4. Añada el usuario no administrador manualmente bajo la clave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\16.0\Secure\ y otórguele acceso de lectura a ella.
5. Añada el usuario no administrador bajo el directorio HKEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring de clave de registro y otórguele permisos completos sobre él.
6. Añada el usuario no administrador bajo el directorio HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib de clave de registro y otórguele acceso de lectura sobre él.
7. Añada el usuario no administrador a la carpeta de instalación de SharePoint Agent (carpeta Candle, por ejemplo, C:\IBM\APM) y otórguele permisos completos sobre ella.
8. Ejecute el mandato **secpol.msc** en **startmenu** para abrir la **Política de seguridad local**.
9. Añada el usuario no administrador a la Política de seguridad local; consulte "Permisos de política de seguridad local" en la página 559
10. Añada el usuario no administrador al grupo de usuarios de Inicio de sesión de SQL Server. El usuario debe tener permisos de rol sysadmin de SQL Server en el servidor SQL.
11. Reinicie el Agente de Microsoft SharePoint Server.
12. Compruebe el estado del Agente de Microsoft SharePoint Server y verifique los datos en el portal de APM.
13. Los siguientes grupos de atributos muestran datos para los usuarios que son miembros del grupo de administradores.
    a) Disponibilidad
    b) Servicio Web

Permisos de política de seguridad local

Hay políticas de seguridad local disponibles para que un usuario no administrador ejecute un Agente de Microsoft SharePoint Server. Estas políticas ayudan a iniciar o detener, configurar y realizar la verificación de datos del agente. Se aplican las dos siguientes políticas de seguridad local para que un usuario no administrador ejecute el Agente de Microsoft SharePoint Server.

Otorgar el permiso Iniciar sesión como servicio
Puede otorgar el permiso Iniciar sesión como servicio.

Acerca de esta tarea
Para otorgar el permiso Iniciar sesión como servicio, siga el procedimiento de Agente de Microsoft SharePoint Server como se describe aquí.

Procedimiento

1. Pulse **Inicio** > **Herramientas administrativas** > **Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.
2. En el panel de navegación, expanda **Política local** y pulse **Asignación de derechos de usuario**. Se abrirá la lista de derechos de usuario.
3. Realice una doble pulsación en la política **Iniciar sesión como servicio**. Se abre la ventana **Propiedades de Iniciar sesión como servicio**.
4. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.

5. En el campo **Especificar los nombres de objeto a seleccionar**, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
6. Pulse **Aceptar**.

Otorgar el permiso Depurar programas
Puede otorgar el permiso Depurar programas.

Acerca de esta tarea
Para otorgar el permiso Depurar programas, siga el procedimiento de Agente de Microsoft SharePoint Server como se describe aquí:

Procedimiento

1. Pulse **Inicio** > **Herramientas administrativas** > **Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.
2. Expanda **Política local** y pulse **Asignación de derechos de usuario**. Se abre la lista de derechos de usuario.
3. Realice una doble pulsación en la política **Depurar programas**. Se abre la ventana **Propiedades de Depurar programas**.
4. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.
5. En el campo Especificar los nombres de objeto a seleccionar, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
6. Pulse **Aceptar**.

Configuración de la supervisión de Microsoft SQL Server

Debe configurar el Monitoring Agent for Microsoft SQL Server para que el agente pueda recopilar datos de la aplicación que se está supervisando.

Antes de empezar

Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Microsoft SQL Server.

Puede instalar y configurar el Agente de Microsoft SQL Server localmente utilizando la interfaz de indicador de mandatos. Asegúrese de que el agente esté instalados en el servidor que se está supervisando.

Acerca de esta tarea

Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte “Historial de cambios” en la página 52.

El Agente de Microsoft SQL Server es un agente de varias instancias; debe configurar e iniciar cada instancia de agente de forma manual.

- Para configurar el agente, realice las tareas siguientes:
  - Crear un usuario y otorgar los permisos necesarios
  - Seleccionar las bases de datos para la supervisión
  - Configurar las variables del entorno local
- Para ejecutar el agente en un entorno de clúster, siga los pasos descritos en el tema "Ejecución del agente en un entorno de clúster".

Cómo crear un usuario y otorgar los permisos

En Microsoft SQL Server, debe crear un usuario en el que se ejecuta el agente y otorgar permisos al usuario para supervisar Microsoft SQL Server. El proceso de otorgar permisos es el mismo para Microsoft SQL Server 2005, o posterior.

Antes de empezar

Instale el Agente de Microsoft SQL Server. Para crear un usuario y otorgarle permisos, debe ser administrador de base de datos con el rol de autorización sysdamin.

Acerca de esta tarea

Utilice el procedimiento siguiente para determinar si un usuario de SQL Server existente tiene permisos suficientes para supervisar Microsoft SQL Server:

- Windows "Comprobación de los permisos de un usuario de SQL Server existente" en la página 561

Utilice uno de los procedimientos siguientes para crear un usuario:

- Windows "Creación de un ID de usuario de SQL Server con autenticación de Windows" en la página 562
- Linux Windows "Creación de un ID de usuario de SQL Server con autenticación de SQL Server" en la página 563

Utilice el procedimiento siguiente para otorgar permisos:

- Windows "Otorgar los permisos necesarios para la recopilación de datos" en la página 563
- Windows "Otorgar permiso a la clave de registro Perflib para recopilar datos para conjuntos de datos nuevos." en la página 565

Comprobación de los permisos de un usuario de SQL Server existente

Windows Puede ejecutar la herramienta de programa de utilidad **koqVerifyPerminssions.exe** para comprobar si un usuario de SQL Server existente tiene permisos suficientes relacionados con bases de datos de SQL Server.

Acerca de esta tarea

La herramienta de programa de utilidad **koqVerifyPerminssions.exe** devuelve el mensaje PASS si el usuario tiene el rol **sysadmin** o los permisos necesarios mínimos. El resultado de la comprobación detallada se registra en `koqVerifyPermissions_log`.

A continuación se indican los permisos mínimos:

- Los permisos para el servidor debe incluir **Ver estado de servidor**, **Ver cualquier base de datos** y **Ver cualquier definición**.

  Estos permisos de nivel de servidor son obligatorios.
- Para todas las bases de datos del sistema y las bases de datos definidas por el usuario para la supervisión, la pertenencia de rol de base de datos debe incluir **public** y **db_owner**.

  El permiso **db_owner** se requiere para recopilar datos para los siguientes conjuntos de datos:
  - Conjunto de datos de detalles de servidor
  - Conjunto de datos de detalles de base de datos
  - Conjunto de datos de duplicación de base de datos
  - Conjunto de datos de resumen de servidor
  - Conjunto de datos de resumen de trabajos
- Para la base de datos **msdb**, la pertenencia de rol de base de datos debe incluir **db_datareader**, **SQLAgentReaderRole** y **SQLAgentUserRole**. Estos permisos son necesarios para el conjunto de datos Detalles de trabajo.

Procedimiento

1. Inicie el indicador de mandatos y vaya al siguiente directorio de programa de utilidad.
   - Para agentes de 64 bits, *inicio_agente*\TMAITM6_x64
   - Para agentes de 32 bits, *inicio_agente* \TMAITM6

   donde *inicio_agente* es el directorio de instalación del agente.
2. Ejecute **koqVerifyPerminssions.exe** proporcionando los parámetros:

   ```
   koqVerifyPermissions.exe -S nombre_instancia -U nombre_usuario -P contraseña
   ```

   Donde:
   - *nombre_instancia* es el nombre de instancia de SQL Server.
   - *nombre_usuario* es el nombre de usuario verificado por la herramienta de programa de utilidad.
   - *contraseña* es la contraseña del usuario. Este parámetro es necesario si se proporciona *nombre_usuario*.

   Nota: Si no se proporciona *nombre_usuario* y *contraseña*, se utiliza el usuario predeterminado que inicia sesión en el sistema. Ejemplo: `NT AUTHORITY\SYSTEM`.

Resultados
El resultado de la comprobación detallada está disponible en `koqVerifyPermissions_log` en el directorio siguiente:

- Para agentes de 64 bits, *inicio_agente*\TMAITM6_x64\logs
- Para agentes de 32 bits, *inicio_agente* \TMAITM6\logs

Donde *inicio_agente* es el directorio de instalación del agente.

Creación de un ID de usuario de SQL Server con autenticación de Windows
Windows Cree un usuario con la autenticación de Windows y asígnele los roles y permisos necesarios.

Procedimiento

Para crear un usuario, realice los pasos siguientes:

1. En **SQL Server Management Studio**, abra **Explorador de objetos**.
2. Pulse ***nombre_instancia_servidor*** > **Seguridad** > **Inicios de sesión**.
3. Pulse con el botón derecho del ratón **Inicios de sesión** y seleccione **Inicio de sesión nuevo**.
4. En el campo **Nombre de inicio de sesión** de la página **General**, escriba el nombre de un usuario de Windows.
5. Seleccione **Autenticación de Windows**.
6. Dependiendo del rol y los permisos que desee asignar a este usuario, complete una de las tareas siguientes:
   - En la página Roles de servidor, asigne el rol *sysadmin* al nuevo ID de inicio de sesión.
   - Si no desea asignar el rol *sysadmin* al usuario, otorgue permisos mínimos al usuario siguiendo los pasos indicados en “Otorgar los permisos necesarios para la recopilación de datos” en la página 563.

   Importante: de forma predeterminada, al nuevo ID de inicio de usuario se le asigna el rol *public*.
7. Pulse **Aceptar**.

Resultados
Se creará un usuario con el rol *public* predeterminado y los permisos que le haya asignado, y se visualizará en la lista **Inicios de sesión**.

Creación de un ID de usuario de SQL Server con autenticación de SQL Server

Linux Windows Cree un usuario con la autenticación de SQL Server y asígnele los roles y permisos necesarios.

Procedimiento

Para crear un usuario, realice los pasos siguientes:

1. En **SQL Server Management Studio**, abra **Explorador de objetos**.
2. Pulse ***nombre_instancia_servidor*** > **Seguridad** > **Inicios de sesión**.
3. Pulse con el botón derecho del ratón **Inicios de sesión** y seleccione **Inicio de sesión nuevo**.
4. En el campo **Nombre de inicio de sesión** de la página **General**, escriba el nombre de un usuario nuevo.
5. Seleccione **Autenticación de SQL Server**.
6. En el campo **Contraseña**, escriba una contraseña para el usuario.
7. En el campo **Confirmar contraseña**, vuelva a escribir la contraseña que ha especificado en el campo **Contraseña**.
8. Dependiendo del rol y los permisos que desee asignar a este usuario, complete una de las tareas siguientes:
   - En la página Roles de servidor, asigne el rol *sysadmin* al nuevo ID de inicio de sesión.
   - Si no desea asignar el rol *sysadmin* al usuario, otorgue permisos mínimos al usuario siguiendo los pasos indicados en "Otorgar los permisos necesarios para la recopilación de datos" en la página 563.

   Importante: de forma predeterminada, al nuevo ID de inicio de usuario se le asigna el rol *public*.
9. Pulse **Aceptar**.

Resultados

Se creará un usuario con el rol *public* predeterminado y los permisos que le haya asignado, y se visualizará en la lista **Inicios de sesión**.

Otorgar los permisos necesarios para la recopilación de datos

Windows Aparte del rol predeterminado **public**, puede asignar el rol **sysadmin** a un usuario u otorgar los permisos mínimos a un usuario de manera que el agente pueda recopilar datos para los conjuntos de datos.

Acerca de esta tarea

Puede otorgar los permisos mediante la interfaz de usuario o la herramienta de programa de utilidad **`permissions.cmd`**.

Procedimiento

- Para otorgar los permisos mínimos al usuario mediante la interfaz de usuario, siga estos pasos:
  a) Abra la página **Roles de servidor** y compruebe que el recuadro de selección **public** esté seleccionado.
  b) Abra la página **Correlación de usuario** y a continuación seleccione los siguientes recuadros de selección para las bases de datos del sistema y las bases de datos definidas por el usuario que desee supervisar:
     – **public**
     – **db_owner**

     Para la base de datos **msdb**, seleccione los siguientes recuadros de selección adicionales:
     – **db_datareader**
     – **SQLAgentReaderRole**

- **SQLAgentUserRole**

c) Abra la página **Securables** y a continuación marque los siguientes recuadros de selección para la instancia de servidor que está supervisando:

- ver base de datos
- ver definición
- ver estado de servidor

- Para otorgar los permisos mínimos al usuario mediante la herramienta de programa de utilidad **permissions.cmd**, realice los pasos siguientes:

a) Inicie el Explorador de Windows y vaya al directorio de la herramienta del programa de utilidad *Agent_grant_perm_dir*:

- Para el agente de 64 bits, *dir_otorg_perm_agente* es *inicio_agente*\TMAITM6_x64\scripts\KOQ\GrantPermission.
- Para el agente de 32 bits, *dir_otorg_perm_agente* es *inicio_agente*\TMAITM6\scripts\KOQ\GrantPermission.
- *inicio_agente* es el directorio de instalación del agente.

Atención: De forma predeterminada, la herramienta del programa de utilidad **permissions.cmd** otorga **db_owner** en todas las bases de datos. Para excluir determinadas bases de datos, debe añadir los nombres de base de datos en el archivo *dir_otorg_perm_agente*\exclude_database.txt. Los nombres de agente deben ir separados por el alias de símbolo **@**.

Consejo: Por ejemplo, si desea excluir las bases de datos **MyDatabase1** y **MyDatabase2**, añada la entrada siguiente en el archivo exclude_database.txt:

```
MyDatabase1@MyDatabase2
```

b) Efectúe una doble pulsación en **permissions.cmd** para iniciar la herramienta del programa de utilidad.

c) Cuando se le solicite, especifique los valores de parámetro que desee:

Tabla 181. Parámetros

Parámetros	**Descripción**
Nombre de SQL Server o nombre de instancia de SQL Server	Especifique el nombre de SQL Server de destino o el nombre de instancia de SQL Server de destino para el que desee otorgar permisos al usuario.
El nombre de inicio de sesión del usuario existente de SQL Server	Especifique el nombre de usuario cuyos permisos se modificarán.
Opciones de los permisos: **1** Otorgar permiso **db_owner** **2** Otorgar permisos **db_datareader**, **SQLAgentReaderRole** y **SQLAgentUserRole** **3** Otorgar todos los permisos necesarios	Especifique **1** o **2** o **3**, según sus requisitos.

Tabla 181. Parámetros (continuación)	
Parámetros	**Descripción**
El usuario al que otorgar permisos: **1** El usuario con la sesión iniciada actualmente en el sistema **2** Otro usuario	Especifique **1** o **2**. Si selecciona **2**, cuando se le solicite especifique el nombre de usuario de destino. **Nota:** Los usuarios deben tener acceso para otorgar permisos a otros usuarios.

Qué hacer a continuación
Configure el agente.

Otorgar permiso a la clave de registro Perflib para recopilar datos para conjuntos de datos nuevos.
Windows Para recopilar datos para unos pocos conjuntos de datos, debe otorgar a los usuarios acceso a la clave de registro Perflib.

Acerca de esta tarea

Debe otorgar este permiso al usuario de Windows con el que se configuran los servicios de agente. Hay muchos conjuntos de datos afectados en ausencia de permisos de Perflib como por ejemplo Detalle de base de datos de MS SQL, Gestor de memoria de MS SQL, Resumen de tipo de recurso de bloqueo de MS SQL, Resumen de trabajo de MS SQL, Resumen de transacciones de servidor de MS SQL, Resumen de servidor MS SQL, etc.

Procedimiento

Para otorgar permiso a la clave de registro Perflib, siga estos pasos:

1. Para abrir el Editor de registro, pulse **Inicio** > **Ejecutar** > **Regedit.exe** y pulse **Intro**.
2. Vaya a la clave de registro `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Perflib`.
3. Pulse con el botón derecho sobre la clave **Perflib** y pulse **Permisos**.
4. Pulse **Añadir**, especifique el nombre de usuario de Windows con el que se ha instalado y configurado el agente y a continuación pulse **Aceptar**.
5. Pulse el usuario que ha añadido.
6. Otorgue acceso de lectura al usuario marcando el recuadro de selección.
7. Pulse **Aplicar** y luego **Aceptar**.

Variables de entorno local

Puede cambiar el comportamiento del Agente de Microsoft SQL Server configurando las variables de entorno local.

Variables para comprobar la disponibilidad del servicio de SQL Server

Para comprobar la disponibilidad del servicio de SQL Server, utilice las siguientes variables de entorno:

- **COLL_MSSQL_RETRY_INTERVAL**: Esta variable proporciona el intervalo de reintento (en minutos) para comprobar el estado de servicio de SQL Server. Si el valor es menor que o igual a cero, la variable toma el valor predeterminado de 1 minuto.
- **COLL_MSSQL_RETRY_CNT**: Esta variable proporciona el número de reintentos que el agente de SQL Server realiza para comprobar si el servicio de SQL Server se ha iniciado o no. Si el servicio de SQL Server no se ha iniciado después del número de reintentos especificado en esta variable, el recopilador deja de funcionar. Si el valor de la variable es menor que o igual a cero, la variable toma el valor predeterminado de infinito.

Variables para supervisar el archivo de registro de errores de SQL Server

Para supervisar el conjunto de datos detalles de sucesos de error de MS SQL, utilice las siguientes variables de entorno:

- **COLL_ERRORLOG_STARTUP_MAX_TIME**: esta variable proporciona el intervalo de tiempo (T) para la recopilación de errores antes del inicio del agente. El valor predeterminado es `0` minutos. Esta variable puede tener los siguientes valores:

  T = 0
  El agente inicia la supervisión del archivo de registro de errores desde el momento en que se inicia o reinicia el agente. El agente no lee los errores que se han registrado en el archivo de registro de errores antes de que se iniciara el agente.

  T = 1
  El agente supervisa el archivo de registro de errores de acuerdo con los valores siguientes establecidos para la variable **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW**, que se representa mediante R:

  - Si R < 0, el agente inicia la supervisión del archivo de registro de errores desde el momento en que se inicia o reinicia el agente.
  - Si R = 1, el agente supervisa todos los errores que se registran en el archivo de registro de errores.
  - Si R > 1 y el agente se instala por primera vez, el agente supervisa el archivo de registro de errores hasta que se supervisan los errores R. Si R > 1 y el agente se reinicia, el agente supervisa todos los errores R omitidos anteriormente.

  T > 1
  El agente supervisa todos los errores anteriores que se han registrado hasta T minutos desde el momento en que el agente se inicia o reinicia. La supervisión de agente también depende de los valores siguientes que se establecen para la variable **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW**:

  - Si R ≤ 0, el agente inicia la supervisión del archivo de registro de errores desde el momento en que se ha iniciado o reiniciado el agente.
  - Si R = 1, el agente supervisa el archivo de registro de errores para todos los errores que se registran hasta T minutos.
  - Si R > 1, el agente no supervisa más de R errores registrados en los últimos T minutos.

- **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW**: esta variable proporciona el número máximo de errores que se deben procesar cuando se inicia el agente. El valor predeterminado es `0`. Puede asignar los valores siguientes a esta variable:

  R = 0
  El agente inicia la supervisión del archivo de registro de errores desde el momento en que se inicia o reinicia el agente. El agente no lee los errores que se han creado en el archivo de registro de errores antes de que se haya iniciado el agente.

  R = 1
  El agente supervisa los errores que se han registrado en los últimos T minutos desde el momento en que se inicia o reinicia el agente.

  R > 1
  El agente supervisa R errores registrados en los últimos T minutos.

- **COLL_ERRORLOG_MAX_EVENT_ROW**: Esta variable proporciona el número de filas de errores. El valor predeterminado es 50. Puede asignar los valores siguientes a esta variable:

  X = 0
  El agente no visualiza los registros de errores.

  X > 0
  El agente muestra las filas de error X.

- **COLL_ERRORLOG_RECYCLE_WAIT**: Esta variable proporciona el intervalo de tiempo (en segundos) durante el que el Agente de Microsoft SQL Server espera antes de recopilar datos del grupo de atributos Detalles de sucesos de error de MS SQL cuando se desencadena la situación en este grupo de atributos. Puede asignar un valor a esta variable en el rango de 1 a 30. Si el valor de esta variable es menor que cero, la variable toma el valor predeterminado de cero (segundos). Si el valor de esta variable es mayor que 30, la variable toma el valor predeterminado de 30 (segundos).

Variable para establecer el intervalo de tiempo de espera de consulta

Para establecer el intervalo del tiempo de espera de consulta para el agente de SQL Server, utilice las siguientes variables de entorno:

- **QUERY_TIMEOUT**: esta variable de entorno define la cantidad máxima de tiempo (en segundos) que el agente de SQL Server espera para recibir una respuesta a una consulta que se envía a SQL Server. El valor de esta variable debe ser inferior a 45 segundos. Sin embargo, si establece el valor para esta variable como 0 segundos, el agente de SQL Server espera indefinidamente para recibir una respuesta de SQL Server. Si el agente de SQL Server accede a muchas bases de datos bloqueadas, debe asignar el valor a esta variable en el rango de 10 – 20 segundos. Si la consulta no se procesa en el intervalo de tiempo de espera establecido, el agente de SQL Server omite la consulta cuyo tiempo de espera ha excedido y pasa a la consulta siguiente de la cola. El agente no visualiza datos para la consulta que ha excedido el tiempo de espera.
- **QUERY_THREAD_TIMEOUT**: esta variable de entorno define la cantidad máxima de tiempo (en segundos) que el agente de SQL Server espera para recibir una respuesta a una consulta que se envía a SQL Server. Esta variable de entorno se aplica a pocos grupos de atributos que utilizan la recopilación de hebras. Por ejemplo: KOQDBD, KOQTBLD, KOQDEVD, etcétera. El valor para esta variable no tiene límite, al contrario que la variable QUERY_TIMEOUT. De lo contrario, funcionaría de igual modo que la variable QUERY_TIMEOUT.

La variable para ver información sobre los trabajos habilitados

Para ver la información sobre trabajos habilitados en el conjunto de datos Detalle de trabajos de MS SQL, utilice la variable de entorno **COLL_JOB_DISABLED**. Si se establece el valor de esta variable como 1, el Agente de Microsoft SQL Server no visualiza información sobre trabajos inhabilitados. Si no especifica esta variable, puede ver información sobre los trabajos habilitados e inhabilitados.

La variable para limitar las filas en el conjunto de datos de Detalle de grupo de archivos de MS SQL

Para limitar el número de filas que el servicio recopilador capta para el conjunto de datos de Detalle de grupo de archivos MS SQL, utilice la variable de entorno **COLL_KOQFGRPD_MAX_ROW**. Esta variable de entorno define el número máximo de filas que el servicio recopilador capta para el conjunto de datos Detalle de grupo de archivos. Si no especifica un valor para esta variable, el servicio de recopilador capta 10.000 filas para el conjunto de datos de Detalle de grupo de archivos. Utilice esta variable de entorno para modificar el límite predeterminado de número máximo de filas en el archivo `koqcoll.ctl`. Realice los pasos siguientes para modificar el límite predeterminado:

1. Especifique el número máximo de filas para KOQFGRPD en el archivo `koqcoll.ctl`.
2. Añada la variable de entorno **COLL_KOQFGRPD_MAX_ROW** y asegúrese de que el valor de esta variable es el mismo que el valor que ha especificado en el archivo `koqcoll.ctl`.

Si el valor en el archivo `koqcoll.ctl` es menor que el valor que se ha especificado en la variable de entorno **COLL_KOQFGRPD_MAX_ROW**, el valor en el archivo `koqcoll.ctl` se trata como el valor del número máximo de filas.

Si el valor en el archivo `koqcoll.ctl` es mayor que el valor que se ha especificado en la variable de entorno **COLL_KOQFGRPD_MAX_ROW**, el valor en la variable de entorno **COLL_KOQFGRPD_MAX_ROW** se trata como el valor del número máximo de filas.

Variables para mejorar la recopilación para el conjunto de datos de Detalle de grupo de archivos de MS SQL

Utilice la variable **COLL_DBD_FRENAME_RETRY_CNT** para especificar el número de intentos que puede hacerse para mover el archivo %COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_ %COLL_SERVERID%__FGRP_TEMP al archivo %COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID %_%COLL_SERVERID%__FGRP_PREV.

Si no especifica un valor para esta variable, el Agente de Microsoft SQL Server hace 3 intentos para mover el archivo.

La variable para limitar las filas en el conjunto de datos de Detalle de dispositivo de MS SQL

Para limitar el número de filas que el servicio recopilador capta para el conjunto de datos de Detalle de dispositivo de MS SQL, utilice la variable de entorno **COLL_KOQDEVD_MAX_ROW**. Esta variable de entorno define el número máximo de filas que el servicio recopilador capta para el conjunto de datos Detalle de dispositivo. Si no especifica un valor para esta variable, el servicio de recopilador capta 10.000 filas para el conjunto de datos de Detalle de dispositivo. Utilice esta variable de entorno para modificar el límite predeterminado de número máximo de filas en el archivo koqcoll.ctl. Realice los pasos siguientes para modificar el límite predeterminado:

1. Especifique el número máximo de filas para KOQDEVD en el archivo koqcoll.ctl.
2. Añada la variable de entorno **COLL_KOQDEVD_MAX_ROW** y asegúrese de que el valor de esta variable es el mismo que el valor que ha especificado en el archivo koqcoll.ctl.

Si el valor en el archivo koqcoll.ctl es menor que el valor que se ha especificado en la variable de entorno **COLL_KOQDEVD_MAX_ROW**, el valor en el archivo koqcoll.ctl se trata como el valor del número máximo de filas.

Si el valor en el archivo koqcoll.ctl es mayor que el valor que se ha especificado en la variable de entorno **COLL_KOQDEVD_MAX_ROW**, el valor en la variable de entorno **COLL_KOQDEVD_MAX_ROW** se trata como el valor del número máximo de filas.

Variables para mejorar la recopilación para el conjunto de datos de Detalle de dispositivo de MS SQL

Para ampliar el conjunto de datos de Detalle de dispositivo de MS SQL, utilice las siguientes variables de entorno:

- **COLL_KOQDEVD_INTERVAL**: Esta variable de entorno le permite especificar un intervalo de tiempo (en minutos) entre dos recopilaciones consecutivas del conjunto de datos de Detalle de dispositivo de MS SQL.

  Nota: De forma predeterminada, la recopilación de datos para el conjunto de datos de Detalle de dispositivo se basa en la demanda. Utilice la variable **COLL_KOQDEVD_INTERVAL** para iniciar una recopilación basada en hebra para el conjunto de datos de Detalle de dispositivo y para establecer el intervalo de tiempo entre dos recopilaciones de hebras.
- **COLL_DBD_FRENAME_RETRY_CNT**: Utilice esta variable de entorno para especificar el número de intentos que se pueden hacer para mover el archivo %COLL_HOME%_tmp_%COLL_VERSION%_ %COLL_SERVERID%_%COLL_SERVERID%__DEVD_TEMP al archivo %COLL_HOME%_tmp_ %COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DEVD_PREV.

Si no especifica un valor para esta variable, el Agente de Microsoft SQL Server hace 1 intento para mover el archivo.

Variables para mejorar la recopilación para el conjunto de datos de Detalle de base de datos de MS SQL

Para ampliar el conjunto de datos de Detalle de base de datos de MS SQL, utilice las siguientes variables de entorno:

- **COLL_KOQDBD_INTERVAL**: Utilice esta variable de entorno para especificar un intervalo de tiempo (en minutos) entre dos recopilaciones basadas en hebras consecutivas del conjunto de datos de Detalle de

base de datos de MS SQL. Si no especifica un valor para esta variable o el intervalo de tiempo especificado es inferior a 3 minutos, Agente de Microsoft SQL Server adopta de forma predeterminado un intervalo de 3 minutos. En caso de que la recopilación tarde más o de que los datos se vean frecuentemente como NOT_COLLECTED, puede comprobar la hora de recopilación haciendo referencia al registro `La recopilación de detalles de base de datos se ha completado en %d segundos` y establecer para la variable un valor superior al tiempo de recopilación especificado en el registro.

- **COLL_DBD_FRENAME_RETRY_CNT**: Utilice esta variable de entorno para especificar el número de intentos que se pueden hacer para mover el archivo `%COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DBD_TEMP` al archivo `%COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DBD_PREV`.

Si no especifica un valor para esta variable, el Agente de Microsoft SQL Server hace 1 intento para mover el archivo.

Variables para mejorar la recopilación para el conjunto de datos de Detalle de auditoría de MS SQL

Para ampliar el conjunto de datos de Detalle de auditoría de MS SQL, utilice las siguientes variables de entorno:

- **COLL_AUDIT_TYPE**: utilice esta variable para habilitar o inhabilitar la supervisión de registros específicos. El valor predeterminado de la variable es [AL][FL][SL]. De forma predeterminada, el agente supervisa los tres tipos de registros: los registros de aplicación, los archivos de auditoría y los registros de seguridad. El valor de la variable incluye dos códigos de caracteres para cada tipo de registro:
  - [AL] para registros de aplicación
  - [FL] para archivos de auditoría
  - [SL] para registros de seguridad

  Puede cambiar el valor de la variable para inhabilitar la supervisión de un tipo de registro específico. Por ejemplo, si especifica el valor de la variable como [AL][SL], los archivos de auditoría no se supervisarán. Si no se especifica ningún valor para la variable, no se supervisarán los detalles de auditoría.
- **COLL_AUDIT_DURATION**: utilice esta variable para informar de los sucesos de auditoría que se han producido durante el intervalo de tiempo que especifique en esta variable. Por ejemplo, si establece esta variable en 7, el conjunto de datos de Detalles de auditoría informa de los sucesos de auditoría que se han producido sólo en las últimas 7 horas. El valor predeterminado de la variable **COLL_AUDIT_DURATION** es `24 horas`.
- **COLL_AUDIT_COLLECTION_INTERVAL**: la recopilación de hebras en el conjunto de datos de Detalles de auditoría proporciona especificaciones de todas las bases de datos que están presentes en la instancia de servidor SQL. Utilice esta variable para establecer el intervalo para esta recopilación de hebras. Por ejemplo, si establece esta variable en 7, se extrae un conjunto nuevo de especificaciones de base de datos de la instancia del servidor SQL después de cada 7 horas. El valor predeterminado de la variable **COLL_AUDIT_COLLECTION_INTERVAL** es 24.

Variable para ampliar la recopilación para el conjunto de datos de Detalle de proceso de MS SQL

Para ampliar la recopilación del conjunto de datos de Detalle de proceso de MS SQL, utilice la variable **COLL_PROC_BLOCK_INTERVAL** con los valores siguientes:

- Si **COLL_PROC_BLOCK_INTERVAL =** `0`, la recopilación para los atributos Duración del bloqueo de proceso y Duración del bloqueo de recurso se inhabilita.
- Si **COLL_PROC_BLOCK_INTERVAL =** *x*, el intervalo entre dos recopilaciones de datos consecutivas para los atributos Duración del bloqueo de proceso y Duración del bloqueo de recurso es *x* minutes.

Si la variable **COLL_PROC_BLOCK_INTERVAL** no está establecido en el directorio `CANDLE_HOME`, el intervalo entre las dos recopilaciones de datos consecutivas es de tres minutos.

Variable para excluir los objetos bloqueados de la recopilación de datos.

Si las consultas que se han enviado para los espacios de trabajo Detalles de base de datos, Detalles de grupo de archivos, Duplicación de bases de datos y Detalles de dispositivo toman mucho tiempo para ejecutarse, utilice la variable **COLL_DBCC_NO_LOCK** para ejecutar una consulta con el valor `WITH (NOLOCK)`. Esta variable hace que la consulta no espere en la cola cuando el objeto en el que se basa la consulta está bloqueado.

Variable para establecer los criterios de clasificación para las filas devueltas por el conjunto de datos de Detalles de tabla

Las filas devueltas por el conjunto de datos de Detalles de tabla se clasifican en orden descendente según el valor que se establece para la variable **COLL_TBLD_SORTBY**. El valor predeterminado para la variable **COLL_TBLD_SORTBY** es FRAG (porcentaje de fragmentación). Los valores válidos son: ROWS (número de filas en una tabla), SPACE (espacio utilizado por la tabla) y OPTSAGE (la edad de las estadísticas del optimizador de la tabla).

Variable para ampliar la recopilación para los conjuntos de datos de Detalle de problema y Resumen de problemas de MS SQL

- **COLL_ALERT_SEV**: utilice esta variable para establecer el nivel de gravedad de los mensajes de error que se muestran en los conjuntos de datos de Detalle de problema y de Resumen de problemas. Los mensajes de error que tienen un nivel de gravedad igual o mayor que el valor indicado en esta variable se visualizan en los conjuntos de datos de Detalle de problema y Resumen de problemas. Por ejemplo, si establecer el valor de esta variable en `10`, los mensajes de error con el nivel de gravedad 10 o superior se muestran en los conjuntos de datos Detalle del programa y Resumen del problema. Si no especifica un valor para esta variable, los mensajes de error con un nivel de gravedad igual o mayor a 17 se muestran en los conjuntos de datos de Detalle de problema y Resumen de problemas.
- **COLL_SINCE_ERRORLOG_RECY**: utilice esta variable para supervisar sólo los errores con gravedad alta en el archivo ERRORLOG actual. Si no especifica un valor para esta variable, el valor de la variable es `0`, lo que significa que para recopilar los datos, el conjunto de datos Resumen de problema también considera los errores de alta gravedad que se leen del archivo ERRORLOG anterior. Para supervisar sólo los errores con gravedad alta en el archivo ERRORLOG actual, establezca el valor de esta variable en 1.

Variables para establecer el valor del intervalo de tiempo de espera

Para establecer el intervalo de tiempo de espera para el Agente de Microsoft SQL Server, puede utilizar las siguientes variables de entorno:

- **WAIT_TIMEOUT**: utilice esta variable para establecer el intervalo de tiempo de espera para el Agente de Microsoft SQL Server. Si algún conjunto de datos tarda más de 45 segundos en recopilar datos, es posible que el agente se cuelgue o algunas situaciones se activen incorrectamente. Consulte si en el registro hay conjuntos de datos que tardan más de 45 segundos en recopilar datos, y utilice la variable **WAIT_TIMEOUT** para aumentar el tiempo de espera entre el proceso de agente y el proceso de recopilador.
- **COLL_DB_TIMEOUT**: utilice esta variable para definir el intervalo de espera (en segundos) para cualquier solicitud, como la ejecución de una consulta en la conexión del servidor SQL existente para que se complete antes de regresar a la aplicación. Si establece este valor en `0`, no hay ningún tiempo de espera. Si no especifica un valor para esta variable, el agente espera 15 segundos antes de regresar a la aplicación.

Variables para establecer las propiedades de los archivos de registro del recopilador

Para establecer las propiedades de los archivos de registro del recopilador, puede utilizar las siguientes variables de entorno:

- **COLL_WRAPLINES**: utilice esta variable para especificar el número máximo de líneas de un archivo `col.out`. El valor predeterminado de esta variable es de 90.000 líneas (aproximadamente 2 MB).

- **COLL_NUMOUTBAK**: utilice esta variable para especificar el número de copias de seguridad de los archivos de registro del recopilador que desea crear. De forma predeterminada, se crean cinco copias del archivo de registro del recopilador. El archivo de copia de seguridad se denomina `*.out`. Cuando este archivo de copia de seguridad está lleno, se le cambia el nombre por `*.ou1` y los últimos registros se graban en el archivo `*.out`. De esta forma, para cinco archivos de copia de seguridad, los registros más antiguos están disponibles en el archivo `*.ou5` y los últimos registros están disponibles en el archivo `*.out`.

  Puede crear más de cinco copias de seguridad de los archivos de registro del recopilador especificando uno de los valores siguientes en la variable **COLL_NUMOUTBAK**:

  – Por menos de 10 archivos de copia de seguridad, especifique el número de archivos de copia de seguridad que desea crear en la variable **COLL_NUMOUTBAK**. Por ejemplo, si especifica 9 en la variable **COLL_NUMOUTBAK**, se crearán nueve archivos de copia de seguridad.
  – Para más de 9 y menos de 1000 archivos de copia de seguridad, en la variable **COLL_NUMOUTBAK** especifique el número de archivos de copia de seguridad precedido por un guión. Por ejemplo, si especifica `-352` en la variable **COLL_NUMOUTBAK**, se crearán trescientos cincuenta dos archivos de copia de seguridad.
- **COLL_DEBUG**: Utilice esta variable para habilitar el rastreo completo del recopilador estableciendo el valor de esta variable en ddddddddddd (10 veces "d").

Variable para suprimir los archivos temporales

COLL_TMPFILE_DEL_INTERVAL: utilice esta variable para especificar el intervalo (en minutos) tras los que deben suprimirse los archivos temporales K0Q_<indicación de fecha y hora>. Si no especifica un valor para esta variable, el valor de la variable es `0`, lo que significa que los archivos temporales se deben suprimir inmediatamente.

Variable para cambiar el controlador utilizado por el agente MS SQL Server

Para cambiar el controlador utilizado por Agente de Microsoft SQL Server, utilice la variable de entorno **KOQ_ODBC_DRIVER**. Esta variable especifica el controlador que Agente de Microsoft SQL Server utiliza para conectar con SQL Server. Si no especifica un valor para esta variable, el agente utiliza ODBC SQL Server Driver como controlador predeterminado.

Nota: Cuando especifica el controlador Microsoft SQL Server, asegúrese de que el nombre de controlador sea correcto y de que el controlador aparezca en la lista de opciones de controlador en el origen de datos (ODBC).

Variable para conectarse a una base de datos de SQL Server habilitada para AlwaysOn

KOQ_APPLICATION_INTENT: utilice esta variable para especificar la opción de conexión al conectarse a SQL Server.
Detalles de la opción **KOQ_APPLICATION_INTENT**:

- **Readonly**: la conexión se abre con **ApplicationIntent** como *readonly*.
- **Readwrite**: la conexión se abre con **ApplicationIntent** como *readwrite*.
  Cuando se establece en Readwrite, el agente de Microsoft SQL Server no realizará ninguna operación de grabación con la conexión.

Si esta variable no se establece, la conexión se establece sin la propiedad **ApplicationIntent**.

Nota: El controlador lo especifica la variable de entorno **KOQ_ODBC_DRIVER**. Si esta variable no se establece, se utiliza el controlador de SQL Server predeterminado.
Si el controlador no da soporte a **ApplicationIntent**, la conexión se abre sin la propiedad **ApplicationIntent**.

Parámetros de configuración del agente

Debe proporcionar los parámetros de configuración obligatorios del agente.

Acerca de esta tarea

La tabla siguiente contiene los detalles de los parámetros de configuración. Revise los parámetros y determine el valor de cada parámetro.

Nombre de parámetro	Descripción	Valor predeterminado	Campo obligatorio
Nombre de usuario	Nombre de usuario o inicio de sesión utilizado para establecer la conexión entre el agente y el servidor SQL	NA	Sí
Contraseña	Contraseña del usuario o inicio de sesión	NA	Sí
Versión de base de datos	Versión de base de datos de SQL Server que debe supervisarse	NA	Sí
Directorio de inicio del servidor de base de datos	Vía de acceso a página de inicio de la base de datos de SQL Server	NA	Sí
Vía de acceso del archivo de registro de errores	Ubicación en la que se encuentra el archivo de registro de errores de SQL Server	NA	Sí

Configuración del agente en sistemas Windows

Puede utilizar la ventana IBM® Cloud Application Performance Management para configurar el agente en sistemas Windows.

Antes de empezar

Antes de configurar el agente, asegúrese de que haya completado las tareas siguientes:

- Crear un usuario y otorgar los permisos necesarios
- Revisar las variables de entorno local

Acerca de esta tarea

El Agente de Microsoft SQL Server es un agente de varias instancias; debe configurar e iniciar cada instancia de agente de forma manual.

- Para configurar el agente, realice las tareas siguientes:
  - Seleccionar las bases de datos para la supervisión
  - Configurar las variables de entorno locales

Seleccionar las bases de datos para la supervisión
Puede seleccionar la base de datos que desea supervisar utilizando la ventana **Configurar agentes de base de datos**.

Procedimiento

1. Abra la ventana **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse la columna **Tarea/Subsistema**, pulse el botón derecho (del ratón) en **Plantilla** y seleccione **Configurar utilizando los valores predeterminados**.
3. En la ventana **Configurar agentes de base de datos**, seleccione el servidor de base de datos que desea supervisar en los **Servidores de base de datos disponibles** y muévalo a la lista **Servidor a supervisar**.
4. En la ventana **Propiedades de servidor de bases de datos**, los valores para los siguientes campos se rellenan automáticamente:

   - Nombre de servidor
   - Versión de base de datos
   - Directorio de inicio
   - Archivo de registro de errores

   Los campos siguientes de la ventana **Propiedades de servidor de bases de datos** son opcionales:

   - Autenticación de Windows
   - Soporte de conexiones de base de datos de larga duración
   - Parámetros ampliados
   - Supervisar todas las bases de datos
   - Frecuencia diaria
   - Frecuencia semanal
   - Frecuencia mensual
   - Hora de inicio de recopilación
   - Recopilación continuada de Detalle de tabla

   Para obtener más información sobre los parámetros de configuración de la ventana **Propiedades de servidor de bases de datos**, consulte "Parámetros de configuración para las propiedades de Database Server" en la página 574.
5. Si no selecciona el campo **Autenticación de Windows**, debe especificar el ID de usuario y la contraseña en los campos **Inicio de sesión** y **Contraseña** utilizando solo caracteres ASCII.
6. En el campo **Parámetros ampliados**, especifique el nombre del conjunto de datos cuya recopilación de datos desea inhabilitar y, a continuación, pulse **Aceptar**.

   Por ejemplo:

   - Escriba `koqtbld` para inhabilitar la recopilación de datos para el conjunto de datos Detalle de tabla.
   - Escriba `koqdbd` para inhabilitar la recopilación de datos para el conjunto de datos Detalle de base de datos.
   - Escriba `koqtbld,koqdbd` para inhabilitar la recopilación de datos para los conjuntos de datos Detalle de tabla y Detalle de base de datos.
7. Si no ha marcado el recuadro de selección **Supervisar todas las bases de datos**, especifique la lista de bases de datos para las que desea habilitar o inhabilitar la supervisión en el campo del área de grupo **Bases de datos**.

   Recuerde: Si marca el recuadro de selección **Supervisar todas las bases de datos** y especifica las bases de datos en el área de grupo **Bases de datos**, el valor del recuadro de selección **Supervisar todas las bases de datos** tiene prioridad.

8. Especifique la frecuencia para la recopilación del conjunto de datos Detalle de tabla de MS SQL. Los valores posibles son diario, semanal o mensual.
9. Marque el recuadro de selección **Recopilación continuada de detalle de tabla** para habilitar la recopilación continua del conjunto de datos Detalle de tabla de MS SQL. Si marca el recuadro de selección **Recopilación continuada de Detalle de tabla**, especifique un valor en el campo **Intervalo entre dos recopilaciones continuas (en minutos)**.
10. En la ventana **Configurar agentes de base de datos**, pulse **Aceptar** y, a continuación, inicie el agente.

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Parámetros de configuración para las propiedades de Database Server
En la ventana **Propiedades de servidor de bases de datos**, puede configurar las propiedades de Database Server, como el nombre, la versión de base de datos y el directorio de inicio.

La tabla siguiente contiene descripciones detalladas de los valores de configuración en la ventana **Propiedades de servidor de bases de datos**.

*Tabla 182. Nombres y descripciones de los valores de configuración en la ventana **Propiedades de servidor de bases de datos***

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos
Nombre de servidor	El nombre de la instancia de Microsoft SQL Server que se debe supervisar. Utilice MSSQLSERVER como el nombre de instancia para la instancia predeterminada. El nombre debe ser lo suficientemente corto para ajustarse al nombre de sistema gestionado, que debe ser de 2 a 32 caracteres longitud.	Sí	Si la instancia de Microsoft SQL Server que se supervisa es la instancia de Microsoft SQL Server predeterminada, introduzca `MSSQLSERVER` en este campo. Si la instancia de Microsoft SQL Server que se supervisa es una instancia con nombre donde el nombre de instancia es `mysqlserver` y el nombre de host es `popcorn`, escriba `mysqlserver` en este campo.

*Tabla 182. Nombres y descripciones de los valores de configuración en la ventana **Propiedades de servidor de bases de datos** (continuación)*

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos
Inicio de sesión	El ID de usuario de Microsoft SQL Server que se debe utilizar para conectarse a Microsoft SQL Server. El ID de usuario es necesario sólo cuando el parámetro **`Windows Authentication`** se establece en `False`. Utilice solo caracteres ASCII para el ID de usuario. Al configurar Agente de Microsoft SQL Server especificando un ID de inicio de sesión en el campo **Inicio de sesión**, el agente utiliza este ID de inicio de sesión para conectarse a Microsoft SQL Server. **Importante:** Mientras se configura el agente, si selecciona el recuadro **Autenticación de Windows** y especifica un ID de inicio de sesión en el campo **Inicio de sesión**, el agente da prioridad a la autenticación de Windows.	No	
Contraseña	Contraseña del ID de usuario Microsoft SQL Server. La contraseña solo es necesaria cuando el parámetro **`Windows Authentication`** se establece en `False`. Utilice solo caracteres ASCII para la contraseña.	No	
Versión de base de datos	Versión de la instancia de SQL Server.	Sí	Las versiones de base de datos para la instancia de SQL Server son las siguientes: • Microsoft SQL Server 2014 - 12.0.2000.8 • Microsoft SQL Server 2012 - 11.0.2100.60 • Microsoft SQL Server 2008 R2 - 10.50.1600.1 • Microsoft SQL Server 2008 - 10.0.1600.22 • Microsoft SQL Server 2005 - 9.0.1399.06

*Tabla 182. Nombres y descripciones de los valores de configuración en la ventana **Propiedades de servidor de bases de datos** (continuación)*

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos
Directorio de inicio	Directorio de instalación de SQL Server.	Sí	La vía de acceso al directorio inicial predeterminado para la instancia de Microsoft SQL Server 2005 predeterminada es `C:\Archivos de programa \Microsoft SQL Server\MSSQL`. Una instancia de Microsoft SQL Server 2005 con nombre tiene una vía de acceso de directorio inicial en el formato `C:\Archivos de programa \Microsoft SQL Server\MSSQL $`*`nombre_instancia`*, donde *nombre_instancia* es el nombre de la instancia de Microsoft SQL Server.

*Tabla 182. Nombres y descripciones de los valores de configuración en la ventana **Propiedades de servidor de bases de datos** (continuación)*

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos
Archivo de registro de errores	La ubicación y el nombre completos del registro de errores de SQL Server.	Sí	La vía de acceso del registro de errores de la instancia de Microsoft SQL Server 2005 predeterminada es `C:\Archivos de programa \Microsoft SQL Server\MSSQL\LOG \ERRORLOG`. Una instancia de Microsoft SQL Server 2005 con nombre tiene una vía de acceso de registro de errores predeterminada con el formato `C:\Archivos de programa \Microsoft SQL Server\MSSQL $`*`nombre_instancia`*`\LOG\ERRORLOG`, donde *nombre_instancia* es el nombre de instancia de Microsoft SQL Server.

*Tabla 182. Nombres y descripciones de los valores de configuración en la ventana **Propiedades de servidor de bases de datos** (continuación)*

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos
Windows Autenticación	La autenticación de Windows es una cuenta de Windows con la que se configuran los servicios de agente y es la opción de configuración predeterminada. Si selecciona el recuadro de selección **Autenticación de Windows**, se utilizan las credenciales de Windows para la autenticación. Cuando Agente de Microsoft SQL Server se configura con la autenticación de Windows, los servicios de agente utilizarán **Cuenta del sistema local** o **Esta cuenta** para iniciar la sesión en el Microsoft SQL Server. • Si los servicios de agente se han configurado para utilizar la **Cuenta del sistema local** para iniciar la sesión, el agente utiliza el ID de usuario NT AUTHORITY\SYSTEM para acceder a Microsoft SQL Server. • Si los servicios de agente se han configurado para utilizar **Esta cuenta** para iniciar la sesión, el agente utiliza el respectivo ID de usuario para acceder a Microsoft SQL Server. **Recuerde:** Si no selecciona el recuadro de selección **Autenticación de Windows**, debe especificar valores para los parámetros de **Inicio de sesión** y **Contraseña**. Si no especifica estos parámetros y pulsa **Aceptar** en la ventana **Propiedades de servidor de bases de datos**, se muestra un mensaje de error en una ventana emergente y la configuración del agente no finaliza. **Importante:** Si configura el agente seleccionando el recuadro de selección **Autenticación de Windows** y especificando un ID de inicio de sesión en el campo **Inicio de sesión**, el agente da prioridad a la autenticación de Windows.	No	
Soporte de conexiones de base de datos de larga duración	Habilita o inhabilita las conexiones de base de datos de larga duración. Los siguientes conjuntos de datos no utilizan conexiones de base de datos de larga duración: • Texto de MS SQL • Detalle de grupos de archivos de MS SQL • Resumen de MS SQL Server	No	

*Tabla 182. Nombres y descripciones de los valores de configuración en la ventana **Propiedades de servidor de bases de datos** (continuación)*

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos
Parámetros ampliados	Inhabilita la recopilación de datos de cualquier grupo de atributos.	No	Por ejemplo: Para inhabilitar la recopilación de datos para el conjunto de datos Detalle de tabla, especifique `koqtbld` en el campo **Parámetros ampliados**. Para inhabilitar la recopilación de datos para el conjunto de datos Detalle de base de datos, escriba `koqdbd` en el campo **Parámetros ampliados**. Para inhabilitar la recopilación de datos para los conjuntos de datos Detalles de tabla y Detalles de base de datos, escriba `koqtbld,koqdbd` en el campo **Parámetros ampliados**.

*Tabla 182. Nombres y descripciones de los valores de configuración en la ventana **Propiedades de servidor de bases de datos** (continuación)*

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos

Base de datos	Para seleccionar las bases de datos para supervisión, especifique un valor para este parámetro. Para habilitar la supervisión de todas las bases de datos que están disponibles en la instancia de servidor SQL, seleccione el recuadro de selección **Supervisar todas las bases de datos** en el área de grupo **Bases de datos**.Por omisión, el recuadro de selección **Supervisar todas las bases de datos** está marcado.
	
	Para habilitar o inhabilitar la supervisión de bases de datos específicas, quita la marca del recuadro de selección **Supervisar todas las bases de datos**.
	• Para supervisar bases de datos específicas, seleccione **Incluir** en la lista, y luego especifique los nombres de las bases de datos en el campo de texto junto a la lista.
	• Para excluir bases de datos específicas de la supervisión, seleccione **Excluir** en la lista, y luego especifique los nombres de las bases de datos en el campo de texto junto a la lista.
	Utilice este campo de texto para filtrar las bases de datos que desee supervisar.
	Para especificar un filtro de base de datos, primero debe seleccionar un separador. Un separador es un carácter que distingue un nombre o una expresión de base de datos de otro.
	Al seleccionar un separador, asegúrese de que los nombres y la expresión de bases de datos no contengan el carácter que se selecciona como separador. No debe usar los caracteres comodín que suelen usarse en la consulta T-SQL (por ejemplo, %, _, [ ], ^, -) si se utilizan en los nombres o la expresión de bases de datos.
	Al especificar filtros de bases de datos:
	• Los nombres de las bases de datos deben empezar con un separador.
	• La expresión de las bases de datos debe empezar con dos separadores.
	La expresión de bases de datos es una expresión válida que se puede utilizar en la parte LIKE parte de la consulta T-SQL. Sin embargo, no puede utilizar la cláusula T-SQL ESCAPE al especificar la expresión de base de datos. Los conjuntos de datos siguientes resultan afectados por el filtro de base de datos: Detalles de base de datos, Resumen de bases de datos, Detalles de dispositivo, Detalles de tabla, Resumen de tablas, Detalles de grupo de archivos, Detalles adicionales de base de datos.
		No	Ejemplos de filtros:
			Caso 1: `% de uso`
			Ejemplo:
			`@@%m%`
			Resultado: se filtran todas las bases de datos que tienen el carácter m en sus nombres.
			Caso 2: `_ uso`
			Ejemplo:
			`@@____`
			Resultado: se filtran todas las bases de datos de una longitud de cuatro caracteres.
			Caso 3: `[] uso`
			Ejemplo:
			`@@[m]___`
			Resultado: se filtran todas las bases de datos de cuatro caracteres y cuyos nombres comienzan con el carácter m.
			Caso 4: `[^] uso`
			Ejemplo:
			`@@[^m]%`
			Resultado: se filtran todas las bases de datos (de cualquier longitud) excepto aquellas cuyos nombres empiecen con el carácter *m*.

*Tabla 182. Nombres y descripciones de los valores de configuración en la ventana **Propiedades de servidor de bases de datos** (continuación)*

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos

Base de datos (continuación)	**Recuerde:**
	• Si no selecciona el recuadro de selección **Supervisar todas las bases de datos**, debe especificar la lista de bases de datos para las que desea habilitar o inhabilitar la supervisión, en el campo de texto que está presente en el área de grupo **Bases de datos**. Si pulsa **Aceptar** en la ventana **Propiedades del servidor de bases de datos** sin seleccionar el recuadro de selección **Supervisar todas las bases de datos** y especificar la lista de bases de datos, se muestra un mensaje de error en una ventana emergente y la configuración del agente no finaliza.
	• Si selecciona el recuadro de selección **Supervisar todas las bases de datos** y también especifica las bases de datos a supervisar en el campo de texto que está presente en el área de grupo **Bases de datos**, se da prioridad al valor del recuadro de selección **Supervisar todas las bases de datos**. La lista de bases de datos que especifique en el campo de texto se ignora.
			Caso 5: entrada errónea
			Ejemplo:
			`@%m%`
			Resultado: no se filtra ninguna de las bases de datos.
			Caso 6: valor predeterminado
			Ejemplo: el campo está en blanco (no se escribe ninguna consulta)
			Resultado: se filtran todas las bases de datos.
			Caso 7: patrones mezclados
			Ejemplo:
			`@@[m-t]_d%`
			Resultado: se filtran todas las bases de datos (de cualquier longitud) cuyos nombres empiezan con los caracteres m, n, o, p, q, r, s, t, seguidos por cualquier carácter, con el carácter d en tercer lugar.

Frecuencia diaria	Utilice esta característica para definir la frecuencia de la recopilación de datos de los atributos Detalle de tabla. Los valores pueden ser de cero a 31.	No	
Frecuencia semanal	Utilice esta característica para especificar un día determinado para recopilar datos para los atributos Detalle de tabla. Los valores pueden ser de cero a siete.	No	
Frecuencia mensual	Utilice esta característica para definir la recopilación de datos de los atributos Detalle de tabla un día determinado del mes. Los valores posibles son 1, 2, 3 y así sucesivamente.	No	

*Tabla 182. Nombres y descripciones de los valores de configuración en la ventana **Propiedades de servidor de bases de datos** (continuación)*			
Nombre de parámetro	**Descripción**	**Campo obligatorio**	**Ejemplos**
Hora de inicio de recopilación	La hora de inicio de recopilación se puede especificar en formato de HH:MM. Los valores posibles para horas son de cero a 23. El valor predeterminado es cero. Los valores posibles para minutos son de cero a 59. El valor predeterminado es cero.	No	
Recopilación continuada de Detalle de tabla	Utilice esta característica para la recopilación continuada, como proceso de fondo, de los datos de Detalle de tabla. De forma predeterminada está marcado el recuadro de selección **Recopilación continuada de Detalle de tabla**.	No	
Intervalo entre dos recopilaciones continuas (en min.)	Especifique el tiempo para el intervalo entre dos recopilaciones en minutos. El intervalo mínimo de tiempo es de 3 minutos. Puede seleccionar el recuadro de selección **Intervalo entre dos recopilaciones continuas (en min.)** o puede utilizar Planificar para especificar la recopilación continua del conjunto de datos Detalle de tabla. Si selecciona el recuadro de selección **Intervalo entre dos recopilaciones continuas (en min.)** debe especificar el intervalo de tiempo para la recopilación. Si utiliza Planificar para especificar la recopilación continua del conjunto de datos Detalle de tabla, el intervalo de tiempo mínimo es de 1 día. El intervalo predeterminado entre dos recopilaciones continuas es de 3 minutos.	No	

El agente recopila los datos en el intervalo de tiempo para el que la recopilación de datos se produce con frecuencia. Por ejemplo, si especifica todas las frecuencias (diarias, semanales y mensuales) para recopilar datos, el agente empieza la recopilación de datos de acuerdo con las siguientes condiciones:

- Si la frecuencia diaria es 7, se seleccionan los valores de frecuencia diaria y se ignoran los valores de frecuencia semanal y mensual.
- Si la frecuencia diaria es > 7, se seleccionan los valores de frecuencia semanal y se ignoran los valores de frecuencia diaria y mensual.

Recuerde: Si está marcado el recuadro de selección **Recopilación continua de Detalle de tabla**, el agente recopila los datos en el intervalo mencionado en el campo **Intervalo entre dos recopilaciones continuas (en min.)** y no de acuerdo con las frecuencias a diario, semanal o mensual.

Configuración de variables de entorno local en sistemas Windows
Puede configurar variables de entorno local para cambiar el comportamiento del Agente de Microsoft SQL Server.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, en el menú **Acciones**, pulse **Avanzada > Editar variables**.
3. En el Monitoring Agent for Microsoft SQL Server: **Alterar temporalmente valores de variables locales**, pulse **Añadir**.
4. En la ventana **Añadir alteración temporal de valor de entorno**, especifique la variable y el valor correspondiente.

   Nota: consulte "Variables de entorno local" en la página 565 para ver la lista completa de variables de entorno configurables.

Ejecución como usuario no administrador
Puede ejecutar el agente de supervisión para Microsoft SQL Server como un usuario no administrador.

Acerca de esta tarea
El Agente de Microsoft SQL Server puede ejecutarse como usuario no administrador desde el grupo Usuarios de dominio.

Procedimiento

1. Inicie la aplicación de Windows Active Directory Users and Computers y cree un usuario de dominio.
   - Asegúrese de que el nuevo usuario sea miembro del grupo *Usuarios del dominio*.
   - Asegúrese de que SQL Server es miembro de *Equipos de dominio*.
2. Añada el usuario de dominio recién creado al grupo de usuarios de *Inicio de sesión de SQL Server*. El usuario de dominio debe tener permiso de rol de **`sysadmin`** SQL Server en el SQL Server o los permisos que se mencionan en https://www.ibm.com/support/knowledgecenter/SSMKFH/com.ibm.apmaas.doc/install/sql_config_agent_grant_permission_sqlserver.htm.
3. Inicie la sesión en SQL Server como administrador de dominio.
4. Otorgue el permiso **Modificar** a todas las unidades a las que accede el Agente de Microsoft SQL Server. Complete los siguientes procedimientos para propagar el permiso a todos los subdirectorios:
   a) Vaya a **Mi PC**.
   b) Pulse la **unidad**.
   c) Pulse la pestaña **Seguridad**.
   d) Añada el usuario creado recientemente.
   e) Otorgue el permiso **Modificar** al usuario recién creado.
   f) Pulse **Aceptar**. Este procedimiento tarda unos pocos minutos en aplicar el permiso a todos los subdirectorios.
5. Utilizando el registro de Windows, otorgue acceso de lectura a `HKEY_LOCAL_MACHINE` y propague los valores. Complete los pasos siguientes para propagar los valores:
   a) Pulse el botón derecho del ratón en el directorio `HKEY_LOCAL_MACHINE` y seleccione **Permisos**.
   b) Añada el usuario creado recientemente.
   c) Seleccione el usuario recientemente creado.
   d) Marque el recuadro de selección **Permitir leer**.
   e) Pulse **Aceptar**. Este procedimiento tarda unos minutos en propagar los valores a todo el árbol de `HKEY_LOCAL_MACHINE`.
6. Utilizando el registro de Windows, otorgue los permisos de registro específicos de agente de acuerdo con la lista siguiente.
   - Si ha instalado un agente de 32 bits en un sistema operativo de 32 bits, otorgue acceso completo al directorio `KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring` y, a continuación, propague los valores.

- Si ha instalado un agente de 32 bits en un sistema operativo de 64 bits, otorgue acceso completo al directorio `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Candle` y, a continuación, propague los valores.
- Si ha instalado un agente de 64 bits en un sistema operativo de 64 bits, otorgue acceso completo al directorio `KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring` y, a continuación, propague los valores.

Complete los pasos siguientes para propagar los valores:

a) Pulse con el botón derecho del ratón el directorio para que tenga acceso completo y seleccione **Permisos**.

b) Añada el usuario creado recientemente.

c) Seleccione el usuario recientemente creado.

d) Marque el recuadro de selección **Permitir control completo**.

e) Pulse **Aceptar**. Este procedimiento tardará unos minutos en propagar los valores a todo el árbol `KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring`.

7. Añada un nuevo usuario del dominio al grupo **Usuarios de supervisor de rendimiento**.
8. Verifique que los Usuarios de dominio sean miembros del grupo *Usuarios*.
9. Otorgue los permisos siguientes al directorio Windows para que se ejecute como un usuario no administrador:
   - Si se instala un agente de 32 bits en un sistema operativo de 32 bits, otorgue acceso de lectura y escritura al directorio `unidad_instalación_SO:\Windows\system32`
   - Si se instala un agente de 32 bits en un sistema operativo de 64 bits, otorgue acceso de lectura y escritura al directorio `unidad_instalación_sistema_operativo:\Windows\SysWOW64`

   Nota: los permisos para el directorio de Windows no son necesarios para Windows Server 2008, Windows Server 2008 R2 y Windows Server 2012, Windows Server 2012 R2, Windows Server 2016.
10. Otorgue el permiso **Modificar** al archivo de registro y al archivo de datos de SQL Server:
    - La vía de acceso predeterminada del archivo de datos de SQL Server es *dir_raíz_SQLServer* `\DATA`, donde *dir_raíz_SQLServer* es el directorio raíz de la instancia de SLQ Server. Por ejemplo, si el directorio raíz de la instancia de SQL Server es `C:\Archivos de programa\Microsoft SQL Server\MSSQL.1\MSSQL`, la vía de acceso de archivo de datos es `C:\Archivos de programa \Microsoft SQL Server\MSSQL.1\MSSQL\DATA`.
    - La vía de acceso predeterminada del archivo de registro de SQL Server es *dir_raíz_SQLServer* `\LOG`, donde *dir_raíz_SQLServer* es el directorio raíz de la instancia de SQL Server. Por ejemplo, si el directorio raíz de la instancia de SQL Server es `C:\Archivos de programa\Microsoft SQL Server\MSSQL.1\MSSQL`, la vía de acceso del archivo de registro es `c:\Archivos de programa\Microsoft SQL Server\MSSQL.1\MSSQL\LOG`.
11. Otorgue permisos completos en el directorio `inicio_Candle`. La vía de acceso predeterminada es `C:\IBM\ITM`.
12. Aplique permisos de seguridad locales; consulte "Permisos de política de seguridad local" en la página 585.
13. Reinicie SQL Server para asegurarse de que los permisos de seguridad locales se aplican de forma eficaz.
14. Cambie los valores de inicio de sesión para los servicios de agente de SQL Server al usuario no administrador completando los pasos siguientes:

    a) Pulse **Inicio > Herramientas administrativas > Servicios**.

    b) Pulse con el botón derecho del ratón **Monitoring Agent For SQL Server *nombre_instancia*** y pulse **Propiedades**. Se abrirá la ventana **Propiedades de Servicio SQL**.

    c) Pulse el separador **Inicio de sesión**.

    d) Pulse **Esta cuenta** y escriba el nombre de usuario.

    e) En los campos **Contraseña** y **Confirmar contraseña**, escriba la contraseña y pulse **Aceptar**.

f) Repita los pasos b hasta e para **Monitoring Agent For SQL Server Collector *nombre_instancia***, donde *nombre_instancia* es el nombre de instancia de Microsoft SQL Server.

Permisos de política de seguridad local

La política de seguridad local administra el sistema y su política de seguridad. Desempeña un papel importante para mantener seguro el agente y el sistema en el que el agente está instalado. Esta política funciona otorgando derechos de acceso y permisos a los usuarios. Para el Agente de Microsoft SQL Server, asegúrese de que el usuario tiene los permisos siguientes para adherirse a la política de permisos de seguridad locales.

Permiso Iniciar sesión como servicio

Acerca de esta tarea

Para otorgar el permiso Iniciar sesión como servicio, realice los pasos siguientes.

Procedimiento

1. Pulse **Inicio > Herramientas administrativas > Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.
2. Pulse **Políticas locales** para expandir la lista.
3. Pulse **Asignación de derechos de usuario**. Se abrirá la lista de derechos de usuario.
4. Realice una doble pulsación en la política **Iniciar sesión como servicio**. Se abre la ventana **Propiedades de Iniciar sesión como servicio**.
5. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.
6. En el campo **Especificar los nombres de objeto a seleccionar**, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
7. Pulse **Aceptar**.

Permiso Depurar programas

Acerca de esta tarea

Para otorgar el permiso Depurar programa, complete el siguiente procedimiento en Agente de Microsoft SQL Server.

Procedimiento

1. Pulse **Inicio > Herramientas administrativas > Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.
2. Pulse **Políticas locales** para expandir la lista.
3. Pulse **Asignación de derechos de usuario**. Se abrirá la lista de derechos de usuario.
4. Realice una doble pulsación en la política **Depurar programas**. Se abrirá la ventana **Propiedades de Depurar programas**.
5. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.
6. En el campo **Especificar los nombres de objeto a seleccionar**, especifique el nombre de la cuenta de usuario a la que desea asignar permisos y, a continuación, pulse **Aceptar**.
7. Pulse **Aceptar**.

Suplantar a un cliente después de la autenticación

Acerca de esta tarea

Para otorgar el permiso Suplantar a un cliente después de la autenticación, siga el procedimiento siguiente en el Agente de Microsoft SQL Server.

Procedimiento

1. Pulse **Inicio > Herramientas administrativas > Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.
2. Pulse **Políticas locales** para expandir la lista.
3. Pulse **Asignación de derechos de usuario**. Se abrirá la lista de derechos de usuario.
4. Realice una doble pulsación en la política **Suplantar a un cliente después de la autenticación**. Se abrirá la ventana **Propiedades de Suplantar a un cliente después de la autenticación**.
5. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.
6. En el campo **Especificar los nombres de objeto a seleccionar**, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
7. Pulse **Aceptar**.

Configuración del agente en sistemas Linux

Para configurar el agente en sistemas operativos Linux, debe ejecutar el script y responder a las solicitudes.

Antes de empezar

Antes de configurar el agente, asegúrese de que haya completado las tareas siguientes:

- Revisar las variables de entorno local

Acerca de esta tarea

El Agente de Microsoft SQL Server es un agente de varias instancias; debe configurar e iniciar cada instancia de agente de forma manual.

Procedimiento

1. En la línea de mandatos, cambie la vía de acceso al directorio de instalación de agente.
   Ejemplo:
   ```
   cd /opt/ibm/apm/agent/bin
   ```
2. Ejecute el mandato siguiente, donde *nombre_instancia* es el nombre que desea proporcionar a la instancia:
   ```
   ./mssql-agent.sh config nombre_instancia
   ```
3. Cuando el indicador de mandatos muestre el siguiente mensaje, escriba 1 y especifique:
   ```
   ¿Desea editar el valor 'Monitoring Agent for MSSQL'? [1=Sí, 2=No]
   ```
4. Especifique valores para los parámetros de configuración cuando se le solicite.
   Para obtener información sobre los parámetros de configuración, consulte la sección Parámetros de configuración del agente.
5. Ejecute el mandato siguiente para iniciar el agente:
   ```
   ./mssql-agent.sh start nombre_instancia
   ```
6. Ejecute el mandato siguiente para detener el agente:
   ```
   ./mssql-agent.sh stop nombre_instancia
   ```

Configuración de variables de entorno locales en sistemas Linux

Puede configurar variables de entorno locales para cambiar el comportamiento del Agente de Microsoft SQL Server.

Procedimiento

1. Inicie un terminal o el gestor de archivos del sistema y cambie al directorio de instalación del agente:
   Ejemplo:

   ```
   /opt/ibm/apm/agent
   ```

2. Ejecute el mandato siguiente para detener el agente:

   ```
   ./mssql-agent.sh stop nombre_instancia
   ```

   Donde *nombre_instancia* es el nombre de instancia de agente.
3. Abra el archivo `.oq.environment` que se encuentra en el directorio de configuración siguiente:
   Ejemplo:

   ```
   dir_instalación/config
   ```

   Donde *dir_instalación* es el directorio de instalación del agente.
4. Añada las variables de entorno necesarias al final del archivo `.oq.environment` siguiendo el formato de pares de nombre y valor.
   `export NOMBRE_VARIABLE=VALOR_VARIABLE`

   Ejemplo:

   ```
   export KOQ_ODBC_DRIVER=ODBC Driver 17 for SQL Server
   ```

   Nota:

   - Consulte “Variables de entorno local” en la página 565 para ver la lista completa de variables de entorno configurables.
   - Las variables personalizadas añadidas no se conservan después de la actualización del agente.
5. Guarde el archivo.
6. Inicie el agente desde el directorio de instalación de agente:

   ```
   cd /opt/ibm/apm/agent/bin
   ```

   ```
   ./mssql-agent.sh start nombre_instancia
   ```

Configuración del agente mediante el archivo de respuestas silencioso

Puede utilizar el archivo de respuestas silencioso para configurar el agente o varias instancias del agente.

Antes de empezar

Para configurar varias instancias del agente, asegúrese de que los detalles de configuración de todas las instancias de agente se especifican en el archivo de respuestas silencioso.

Acerca de esta tarea

Ejecute el script de configuración para cambiar los valores de configuración. Puede editar el archivo de respuestas silencioso antes de ejecutar el script de configuración.

Procedimiento

Para configurar el agente, realice los pasos siguientes:

1. Inicie un editor de texto y abra el archivo de respuestas silencioso que está disponible en la ubicación siguiente:
   - Windows *dir_instalación*\samples/mssql_silent_config.txt
   - Linux *dir_instalación*/samples/mssql_silent_config.txt

Donde *dir_instalación* es el directorio de instalación del agente.

Ejemplo:

- Windows `C:\IBM\APM\samples\mssql_silent_config.txt`
- Linux `/opt/ibm/apm/agent/samples/mssql_silent_config.txt`

Nota: Para obtener información sobre los parámetros de configuración del agente, consulte "Parámetros de configuración del agente " en la página 571.

2. Inicie un indicador de mandatos y cambie al directorio siguiente:
   - Windows
     ```
     cd dir_instalación\bin
     ```
   - Linux
     ```
     cd dir_instalación/bin
     ```
3. Ejecute el mandato siguiente:
   - Windows
     ```
     mssql-agent.bat config dir_instalación\samples\mssql_silent_config.txt
     ```
   - Linux
     ```
     mssql-agent.sh config  nombre_instancia dir_instalación/samples/mssql_silent_config.txt
     ```
4. Inicie el agente.
   - Windows En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón la instancia de agente que ha creado y pulse Iniciar.
   - Linux Ejecute el mandato siguiente:
     ```
     cd /opt/ibm/apm/agent/bin
     ```
     ```
     ./mssql-agent.sh start nombre_instancia
     ```

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Ejecución del agente en un entorno de clúster

Windows Puede configurar el Agente de Microsoft SQL Server en un entorno de clúster. Varias instancias de Microsoft SQL Server y del Agente de Microsoft SQL Server pueden ejecutarse en un solo nodo.

Tras instalar y configurar el Agente de Microsoft SQL Server, realice las tareas siguientes para ejecutar el agente en un entorno de clúster:

- Añadir variables de entorno
- Cambiar el tipo de inicio del servicio de agente y del servicio de recopilador
- Añadir el agente y el recopilador al entorno de clúster

Puede configurar un entorno de clúster para las versiones siguientes de Microsoft SQL Server:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016

Importante: en sistemas Windows, el agente debe instalarse en el mismo directorio donde se ha instalado el agente del sistema operativo. Instale el agente en el disco del sistema de los nodos de cada nodo de clúster.

Adición de variables de entorno
Debe configurar las variables de entorno utilizadas por los agentes instalados en cada nodo de clúster.

Acerca de esta tarea
Debe especificar valores para las siguientes variables de entorno:

- *CTIRA_HOSTNAME*: esta variable se utiliza para configurar cada instancia del Agente de Microsoft SQL Server. El valor de esta variable está limitado a 31 caracteres y es común para todos los agentes de supervisión. Establezca el valor de esta variable en el nombre de clúster al que deben navegar todos los agentes de supervisión para ese clúster en el Panel de instrumentos del rendimiento de aplicaciones.
- *CTIRA_NODETYPE*: esta variable se utiliza para identificar el agente. De forma predeterminada, el valor de esta variable se establece en **MSS** para el Agente de Microsoft SQL Server.
- *CTIRA_SUBSYSTEMID*: esta variable se utiliza para distinguir las diversas instancias del Agente de Microsoft SQL Server. De forma predeterminada, el valor de esta variable se establece en **Microsoft SQL Virtual Server** para el Agente de Microsoft SQL Server.
- *COLL_HOME*: esta variable se utiliza para recopilar datos y almacenar archivos de registro para grupos de atributos que utilizan archivos de configuración en una ubicación compartida. Establezca el valor de la variable en *X*:\shared-location, donde *X* es la unidad compartida accesible para los nodos del clúster. Por ejemplo, establezca el valor de la variable *COLL_HOME* al definir los valores de configuración para los grupos de atributos Detalles de tabla de MS SQL o Detalles de sucesos de error de MS SQL.
- *CTIRA_HIST_DIR*: esta variable se utiliza para especificar la vía de acceso al directorio de disco compartido. Si el historial del Agente de Microsoft SQL Server está configurado para almacenarse en el agente de supervisión, cada instancia del agente debe configurarse con una variable *CTIRA_HIST_DIR* común que haga referencia al directorio de disco compartido.

  Recuerde: si el historial se almacena en el Servidor de Cloud APM, no necesita especificar un valor para la variable *CTIRA_HIST_DIR*. El almacenamiento del historial en el Servidor de Cloud APM aumenta la carga en ese servidor.

Para añadir estas variables, siga los pasos descritos en la sección "Configuración de variables de entorno local en sistemas Windows" en la página 582.

Qué hacer a continuación
Cambie el tipo de inicio del servicio de agente y del servicio de recopilador a **Manual** siguiendo los pasos descritos en la sección "Cambio del tipo de inicio del servicio de agente y del servicio de recopilador" en la página 589.

Cambio del tipo de inicio del servicio de agente y del servicio de recopilador
De forma predeterminada, el tipo de inicio del servicio de agente y del servicio de recopilador es **Automático**. Cambie el tipo de inicio del servicio de agente y del servicio de recopilador a **Manual** para que el recurso de clúster pueda controlar el inicio y detención del agente de supervisión.

Procedimiento

Para cambiar el tipo de inicio del servicio de agente, realice los pasos siguientes:

1. Pulse **Inicio** > **Ejecutar**, especifique el mandato `services.msc` y pulse **Aceptar**.
2. Pulse el agente con el botón derecho del ratón y pulse **Propiedades**.
3. En la ventana **Propiedades de Monitoring Agent for Microsoft SQL Server**, en la lista **Tipo de inicio**, seleccione **Manual**, pulse **Aplicar** y luego **Aceptar**.

Qué hacer a continuación

- Siga el mismo procedimiento para cambiar el tipo de inicio del servicio de recopilador a **Manual**.
- Añada el agente y el recopilador al entorno de clúster siguiendo los pasos descritos en la sección "Adición del agente y el recopilador al entorno de clúster " en la página 590.

Adición del agente y el recopilador al entorno de clúster
Debe añadir el agente y el recopilador al entorno de clúster.

Procedimiento

1. Pulse **Inicio > Panel de control > Herramientas administrativas > Failover Cluster Management**.
2. Expanda **Failover Cluster Management**.
3. Expanda **Servicios y aplicaciones** y pulse con el botón derecho del ratón la instancia de SQL que desee configurar.
4. Pulse **Añadir un recurso > Servicio genérico**. Se abre el Asistente de Nuevo recurso.
5. En la página Seleccionar servicio, seleccione el nombre del servicio y pulse **Siguiente**.

   Ejemplos de nombres de servicios de Windows:

   - `Monitoring Agent for Microsoft SQL Server: SQLTEST#INSTANCE1`
   - `Monitoring Agent for Microsoft SQL Server: Collector SQLTEST#INSTANCE1`
   - `Monitoring Agent for Microsoft SQL Server: SQLTEST2#INSTANCE2`
   - `Monitoring Agent for Microsoft SQL Server: Collector SQLTEST2#INSTANCE2`
6. En la página Confirmación, compruebe los detalles y pulse **Siguiente**.
7. En la página Resumen, pulse **Finalizar**. Ahora se ha añadido el Agente de Microsoft SQL Server.

   Recuerde: siga los mismos pasos para añadir el recopilador al entorno de clúster.
8. Para situar el agente en línea, púlselo con el botón derecho del ratón y pulse **Situar este recurso en línea**.
9. Para situar el recopilador en línea, púlselo con el botón derecho del ratón y pulse **Situar este recurso en línea**.

Resultados
El Agente de Microsoft SQL Server está ahora en ejecución en un entorno de clúster.

Recuerde: si desea volver a configurar el agente, primero debe situar el agente y el recopilador fuera de línea, o editar las variables del agente en el nodo donde se ejecutan el agente y el recopilador. Una vez finalizada la configuración del agente, vuelva a situar en línea el agente y el recopilador.

Configuración del agente utilizando el programa de utilidad de clúster

Windows Puede utilizar el programa de utilidad de clúster para añadir varias instancias del Agente de Microsoft SQL Server en un grupo de clústeres de un entorno de clústeres.

El programa de utilidad de clúster añade el servicio de agente y el servicio recopilador de cada instancia del Agente de Microsoft SQL Server como recurso de servicio genérico en el grupo de clústeres. Puede utilizar el programa de utilidad de clúster para completar las tareas siguientes:

- Adición de una instancia de SQL Server a un clúster
- Actualización de una instancia existente de agente de SQL Server en un clúster
- Eliminación de una instancia de agente de SQL Server desde un clúster

Requisitos previos para utilizar el programa de utilidad de clúster
Debe asegurarse de que su entorno de sistema cumple los requisitos previos para así poder ejecutar el programa de utilidad de clúster.

Asegúrese de que se cumplen los requisitos previos siguientes:

- Ejecutar el programa de utilidad de clúster en un sistema que tiene como mínimo un grupo en el entorno de clúster.
- Iniciar el servicio de registro remoto de todos los nodos en el clúster.
- Debe tener la autorización de gestor de clúster para acceder al programa de utilidad de clúster.
- El nombre de servicio del agente y del recopilador deben ser los mismos en todos los nodos de clúster.

  Por ejemplo, si el nombre de servicio de agente es Monitoring Agent for Microsoft SQL Server: SQLTEST#INSTANCE1 y el nombre del recopilador es Monitoring Agent for Microsoft SQL Server: Recopilador SQLTEST#INSTANCE1, entonces debe existir el mismo nombre de servicio en todos los nodos del clúster.

Adición de una instancia del Agente de Microsoft SQL Server al clúster
Puede utilizar el programa de utilidad de clúster para añadir una instancia del Agente de Microsoft SQL Server en un grupo de clústeres de un entorno de clústeres.

Procedimiento

1. Para ejecutar el programa de utilidad, realice uno de los pasos siguientes:
   - Para un agente de 64 bits, vaya al directorio *candle_home*\TMAITM6_x64.
   - Para un agente de 32 bits, vaya al directorio *candle_home*\TMAITM6.
2. Para ejecutar el programa de utilidad de clúster, haga doble clic en KoqClusterUtility.exe.
3. En el área SQL **Instancias disponibles del agente de servidor**, seleccione una instancia del Agente de Microsoft SQL Server y pulse **Añadir**.
4. En la ventana **Seleccionar nombre de grupo de clústeres**, seleccione un grupo de clústeres.

   El grupo de clústeres que seleccione debe ser la instancia de SQL Server que supervisa el Agente de Microsoft SQL Server.
5. En la ventana **Seleccione ruta de ubicación compartida**, vaya a la vía donde se almacenan los registros de recopilador y el agente.

   Si no selecciona la vía de acceso, se selecciona de forma predeterminada la ubicación CANDLEHOME/TMAITM6(_x64)/logs para almacenar el agente y los registros de recopilador.
6. Para añadir la instancia del Agente de Microsoft SQL Server al entorno de clústeres, pulse **Aceptar**.

   El panel **Historial** mostrará los registros de actividad del programa de utilidad del clúster.

Actualización de una instancia existente del Agente de Microsoft SQL Server en un clúster.
Puede utilizar el programa de utilidad de clúster para actualizar la ubicación donde se almacenan los registros del agente y del recopilador para una instancia de SQL Server en un clúster.

Procedimiento

1. Para actualizar una instancia Agente de Microsoft SQL Server existente, abra la ventana **Programa de utilidad de clúster**.
2. En el área **Instancias configuradas del agente de SQL Server**, seleccione una instancia del Agente de Microsoft SQL Server y pulse **Actualizar**.
3. En la ventana **Configurar vía para la ubicación compartida**, vaya a la vía donde se almacenan los registros de recopilador y el agente.

   Si no selecciona la vía de acceso, los registros del agente y del recopilador se almacenarán en la ubicación que se haya establecido cuando se añadió la instancia del Agente de Microsoft SQL Server en un clúster.
4. Pulse **Aceptar**.

El panel **Historial** mostrará los registros de actividad del programa de utilidad del clúster.

Eliminación de una instancia dek Agente de Microsoft SQL Server de un clúster
Puede utilizar el programa de utilidad del clúster para eliminar una instancia del Agente de Microsoft SQL Server de un grupo de clústeres.

Procedimiento

1. Abra la ventana **Programa de utilidad de clúster**.
2. En el área **Instancias configuradas del agente de SQL Server**, seleccione una instancia del Agente de Microsoft SQL Server y pulse **Eliminar**.
3. En el cuadro de diálogo **Confirme acción**, pulse **Sí** para suprimir la instancia del Agente de Microsoft SQL Server del clúster.

   El panel **Historial** mostrará los registros de actividad del programa de utilidad del clúster.

Configuración de varias ordenaciones para el archivo ERRORLOG

Agente de Microsoft SQL Server versión 06.31.17.00 o posterior para Application Performance Management versión 8.1.4.0.4 da soporte a varias ordenaciones en el archivo ERRORLOG. Ahora puede configurar el agente para analizar más de una ordenación en el archivo ERRORLOG para el grupo de atributos **Detalle de problema**. Tenga en cuenta que las distintas ordenaciones en el archivo ERRORLOG no son aplicables al grupo de atributos **Detalle de sucesos de error**.

Antes de empezar

Para configurar varias ordenaciones del agente, asegúrese de que el agente esté instalado.

Acerca de esta tarea
La ordenación predeterminada es en inglés. Para otros idiomas de SQL Server, el agente analizará el archivo ERRORLOG según las ordenaciones del archivo de configuración koqErrConfig.ini. Por lo tanto, debe añadir las ordenaciones que se utilizan en el archivo koqErrConfig.ini.

Procedimiento

Para configurar varias ordenaciones para el agente, realice los pasos siguientes:

1. Vaya al directorio del agente *directorio_agente*.

   Windows

   - Para el agente de 64 bits, *directorio_agente* es *inicio_agente*\TMAITM6_x64.
   - Para el agente de 32 bits, *directorio_agente* es *inicio_agente*\TMAITM6.

   Linux

   - Para el agente de 64 bits, *directorio_agente* es *inicio_agente*/TMAITM6_x64.

   Donde *inicio_agente* es el directorio de instalación del agente.
2. Abra el archivo de configuración koqErrConfig.ini:
3. Vaya al final del archivo para añadir las nuevas ordenaciones.

   Por ejemplo, para habilitar la ordenación para francés, añada los siguientes valores de ordenación con el formato de par **nombre-valor** al final del archivo koqErrConfig.ini.

   ```
   [French]
   Error = Erreur :
   Severity = Gravité :
   State = État :
   ```

   Nota: La lista de ejemplo de ordenaciones está disponible en *directorio_agente* \koqErrConfigSample.ini.

   Donde Windows

- Para el agente de 64 bits, *directorio_agente* es *inicio_agente*\TMAITM6_x64.
- Para el agente de 32 bits, *directorio_agente* es *inicio_agente*\TMAITM6.

Linux

- Para el agente de 64 bits, *directorio_agente* es *inicio_agente*/TMAITM6_x64.

Donde *inicio_agente* es el directorio de instalación del agente.

Si la ordenación de destino no está disponible en koqErrConfigSample.ini, puede determinar los valores de palabra clave de ordenación a partir del archivo ERRORLOG.
Siga el siguiente formato de ordenación cuando configure los valores de ordenación en koqErrConfig.ini.

```
[nombre_sección]
Error = valor_error
Severity = valor_gravedad
State = valor_estado
```

Donde

- *nombre_sección* es el nombre de ordenación de SQL Server. Asegúrese de que el nombre de ordenación esté entre un corchete de apertura "**[**" y un corchete de cierre "**]**".
- *valor_error* es la palabra clave de error correspondiente que se encuentra en el archivo ERRORLOG de la ordenación de destino.
- *valor_gravedad* es la palabra clave de gravedad correspondiente que se encuentra en el archivo ERRORLOG de la ordenación de destino.
- *valor_estado* es la palabra clave de estado correspondiente que se encuentra en el archivo ERRORLOG de la ordenación de destino.

Importante: Los valores de palabra clave deben ser los mismos que los valores de palabra clave que se encuentran en el archivo ERRORLOG, incluidos los caracteres especiales.

4. Guarde el archivo de configuración koqErrConfig.ini.

   No es necesario reiniciar el agente.

   Si el archivo de configuración koqErrConfig.ini no está disponible o el archivo de configuración koqErrConfig.ini está vacío, el archivo ERRORLOG mostrará la ordenación predeterminada como un mensaje de error en inglés con nivel de gravedad superior al nivel de gravedad predeterminado, si lo hay.

   Si el archivo de configuración koqErrConfig.ini está configurado correctamente, el archivo ERRORLOG mostrará los mensajes de error correspondientes con nivel de gravedad superior al nivel de gravedad predeterminado, si lo hay.

   El nivel de gravedad predeterminado es 17.

   Atención: Los cambios realizados en el archivo koqErrConfig.ini no se conservan durante la actualización del agente. Debe hacer una copia de seguridad antes de actualizar el agente.

Qué hacer a continuación
Compruebe el widget **Alerta de registro cronológico de errores** o el grupo de atributos **Detalle de problema** o el panel de instrumentos de Application Performance Management como el resultado de los valores de ordenación.

Configuración de la supervisión de MongoDB

Monitoring Agent for MongoDB requiere un nombre de instancia. Debe configurar e iniciar la instancia de agente manualmente. El Agente de MongoDB da soporte a la supervisión local y remota. Consulte los requisitos siguientes para configurar el Agente de MongoDB para la supervisión remota y local.

Antes de empezar

- Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, Software Product Compatibility Reports (SPCR) para el Agente de MongoDB.
- Asegúrese de que el usuario que configura el Agente de MongoDB, tiene los roles necesarios para recopilar datos para todos los atributos.
  - Para configurar el agente en la base de datos MongoDB versión 2.4 y versión 2.6, deben asignarse al usuario los roles clusterAdmin, readAnyDatabase y dbAdminAnyDatabase.
  - Para configurar el agente en la base de datos MongoDB versión 3.x y 4.x, deben asignarse al usuario los roles clusterMonitor, readAnyDatabase y dbAdminAnyDatabase.

  Para conocer los grupos de atributos para los que son necesarios estos roles, consulte Tabla 183 en la página 594.
- Utilice un usuario existente o cree un usuario en la base de datos admin.

  Importante: Para poder crear un usuario y otorgarle los roles adecuados, debe conectar con la base de datos MongoDB y cambiar la base de datos por la base de datos admin. Si el proceso mongod o mongos se está ejecutando en la modalidad de autenticación, especifique las credenciales necesarias para conectar con la base de datos MongoDB.

  1. Ejecute el mandato siguiente para conectar con la base de datos MongoDB:

     `mongo IP:puerto`

     Donde

     - *IP* es la dirección IP del proceso mongod o mongos
     - *puerto* es el número de puerto del proceso de mongod o mongos
  2. Cambie la base de datos por la base de datos admin:

     use admin
  3. Ejecute uno de los siguientes mandatos para añadir un usuario en la base de datos MongoDB y asígnele los roles necesarios al usuario:
     - Para la base de datos MongoDB versión 2.4, ejecute el siguiente mandato:

       ```
       db.addUser({ user: "nombre_usuario", pwd: "contraseña", roles:
       [ 'clusterAdmin', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })
       ```
     - Para la base de datos MongoDB versión 2.6, ejecute el siguiente mandato:

       ```
       db.createUser({user: "nombre_usuario", pwd: "contraseña", roles:
       [ 'clusterAdmin', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })
       ```
     - Para la base de datos MongoDB versión 3.x y 4.x, ejecute el siguiente mandato:

       ```
       db.createUser({user: "nombre_usuario", pwd: "contraseña", roles:
       [ 'clusterMonitor', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })
       ```
  4. Ejecute el siguiente mandato para verificar que el usuario se añade a la base de datos admin.

     `db.auth("nombre_usuario", "contraseña")`

     El código de retorno **1** indica que el usuario se añade, mientras que el código de retorno **0** indica que la adición de usuario ha fallado.

La tabla siguiente contiene información sobre los roles de usuario y los atributos para los que estos roles son necesarios:

Tabla 183. Grupos de atributos y sus roles de usuario necesarios

Roles	Versión de base de datos MongoDB	Grupos de atributos
dbAdminAnyDatabase	2.x, 3.x y 4.x	Tiempos de respuesta

Tabla 183. Grupos de atributos y sus roles de usuario necesarios (continuación)

Roles	Versión de base de datos MongoDB	Grupos de atributos
readAnyDatabase	2.x, 3.x y 4.x	• Listado de Mongod • Información de fragmento general • Almacenamiento de recopilación • Nombres de base de datos • Detalles de fragmento • Detalles de almacenamiento de recopilación
clusterAdmin	2.x, 3.x y 4.x	• Información de instancia de Mongo • Información de E/S de instancia de Mongo • Copia de MII para APMUI uno • Copia de MII para APMUI dos • Bloqueo de base de datos de instancia de Mongo • Bloqueos • Bloqueos de MongoDB • Detalles de WiredTiger • Detalles de MMAPv1
clusterMonitor	2.x, 3.x y 4.x	• Información de instancia de Mongo • Información de E/S de instancia de Mongo • Copia de MII para APMUI uno • Copia de MII para APMUI dos • Bloqueo de base de datos de instancia de Mongo • Bloqueos • Bloqueos de MongoDB • Detalles de WiredTiger • Detalles de MMAPv1

- Para la supervisión remota del servidor MongoDB, consulte los dos requisitos previos

  1. Puesto que Agente de MongoDB requiere el shell de mongo para recopilar información de forma remota desde el servidor MongoDB, el sistema en el que Agente de MongoDB está instalado y configurado debe tener una instancia del servidor MongoDB. El shell de mongo del servidor MongoDB en la máquina agente se utiliza para conectarse al servidor MongoDB remoto para la supervisión.
  2. En el archivo `/etc/hosts` del sistema que aloja el agente, debe haber una entrada de la máquina remota.

Acerca de esta tarea

El nombre de sistema gestionado incluye el nombre de instancia que especifique. Por ejemplo, puede especificar el nombre de instancia como *nombre_instancia*:*nombre_host*:*pc*, donde *pc* es el código de producto de dos caracteres de su agente. El nombre de sistema gestionado puede contener hasta 32 caracteres. El nombre de instancia puede contener hasta 28 caracteres, excluida la longitud del nombre de host. Por ejemplo, si especifica Mongo2 como nombre de instancia, el nombre de sistema gestionado será Mongo2:hostname:KJ.

Importante: Si especifica un nombre de instancia largo, el nombre de sistema gestionado queda truncado y el código de agente no se visualiza correctamente.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Recuerde:

- Para que el agente recopile datos satisfactoriamente, inícielo con el superusuario (root) o utilice el mismo ID de usuario para iniciar el agente y el proceso mongod.
- En un entorno en el que MongoDB se ejecuta como un clúster, asegúrese de instalar el agente en el mismo sistema en el que se está ejecutando el proceso de direccionador. Configure el agente en el mismo sistema con la dirección IP y el número de puerto de ese sistema y la configuración **TYPE** como 1.
- En un entorno en el que MongoDB se ejecuta como un clúster en modalidad de autenticación, asegúrese de añadir el mismo ID de usuario con los derechos necesarios sobre todos los fragmentos del clúster.

Puede configurar el agente utilizando los valores predeterminado, editando el archivo de respuestas silencioso o respondiendo a solicitudes.

Configuración del agente con valores predeterminados

Para un entorno típico, utilice los valores predeterminados para configurar el agente. Si se utilizan los valores predeterminados para la configuración del agente, éste no se ejecuta en modo de autenticación.

Procedimiento

1. Ejecute el mandato siguiente:
   dir_instalación/bin/mongodb-agent.sh config *nombre_instancia*
   dir_instalación/samples/mongodb_silent_config.txt

   Donde

   - *nombre_instancia* es el nombre que se especifica para la instancia de aplicación exclusiva.
   - *dir_instalación* es el directorio de instalación de Agente de MongoDB.

   El directorio de instalación predeterminado es /opt/ibm/apm/agent.
2. Ejecute el mandato siguiente para iniciar el agente:
   dir_instalación/bin/mongodb-agent.sh start *nombre_instancia*

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración y configurar el agente.

Antes de empezar

Para ejecutar la base de datos MongoDB en modalidad de autenticación, asegúrese de configurar el agente con un usuario que tiene los roles clusterAdmin, readAnyDatabase y dbAdminAnyDatabase en la base de datos MongoDB.

Procedimiento

1. En un editor de texto, abra el archivo de respuestas silencioso que está disponible en la siguiente vía de acceso:
   dir_instalación/samples/mongodb_silent_config.txt.
2. Para el parámetro **TYPE**, escriba uno de los siguientes valores:
   - 1 para un clúster
   - 2 para un conjunto de réplicas
   - 3 para una instancia autónoma

   De forma predeterminada, el agente supervisa un clúster.
3. En el parámetro **PORT**, especifique el número de puerto del direccionador de un clúster MongoDB o una instancia mongod del conjunto de réplicas MongoDB que se esté supervisando.

   Recuerde: Si no especifica ningún número de puerto, el agente descubre automáticamente el número de puerto del proceso MongoDB adecuado que está activo en la interfaz por omisión. Si no hay ningún proceso de MongoDB activo en la interfaz por omisión, el agente selecciona el número de puerto del proceso MongoDB adecuado que está activo en la interfaz secundaria.
4. Para el parámetro **HOST**, especifique la dirección IP del sistema host de MongoDB.

   Recuerde: Si no especifica ninguna dirección IP, el agente detecta automáticamente la dirección IP del proceso MongoDB adecuado que está activo en la interfaz por omisión. Si no hay ningún proceso de MongoDB activo en la interfaz por omisión, el agente detecta la dirección IP del proceso MongoDB adecuado que está activo en la interfaz secundaria.
5. En el parámetro **AUTHENTICATION**, especifique YES para indicar que mongoDB se ejecuta en modo de autenticación. El valor predeterminado es NO, que indica que el agente no se ejecuta en modo de autenticación.

   Recuerde: Cuando la base de datos MongoDB se está ejecutando en modalidad de autenticación, el Agente de MongoDB o cualquier cliente de MongoDB no se puede conectar a la base de datos de MongoDB sin credenciales. Para conectar con la base de datos que se ejecuta en la modalidad de autenticación, especifique YES para el parámetro **AUTHENTICATION**.

   Si especifica YES, realice los pasos siguientes:

   a) Para el parámetro **Nombre de usuario**, especifique un nombre de usuario para el direccionador o la instancia de mongod. Asegúrese de que se asignan los roles mínimos al usuario. Para obtener información sobre los roles de usuario, consulte Tabla 183 en la página 594.

   b) En el parámetro **Contraseña**, especifique la contraseña.
6. Guarde y cierre el archivo mongodb_silent_config.txt y ejecute el mandato siguiente:
   dir_instalación/bin/mongodb-agent.sh config *nombre_instancia*
   dir_instalación/samples/mongodb_silent_config.txt

   Donde

   - *nombre_instancia* es el nombre que se especifica para la instancia.
   - *dir_instalación* es el directorio de instalación de Agente de MongoDB.
7. Ejecute el mandato siguiente para iniciar el agente:

dir_instalación/bin/mongodb-agent.sh start *nombre_instancia*

Importante: Si actualiza el agente a V1.0.0.9 o posterior, y desea ejecutar el agente en modalidad de autenticación, deberá volver a configurar el agente para proporcionar un nombre de usuario y una contraseña. Para recopilar datos, debe detener y reiniciar el agente después de la configuración.

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente respondiendo a solicitudes

Para configurar el agente con valores personalizados, puede especificar valores para los parámetros de configuración cuando se le solicite mientras se está ejecutando el script.

Procedimiento

1. Ejecute el mandato siguiente:
   dir_instalación/bin/mongodb-agent.sh config *nombre_instancia*

   Donde

   - *nombre_instancia* es el nombre que se especifica para la instancia.
   - *dir_instalación* es el directorio de instalación de Agente de MongoDB.
2. Cuando se le solicite que proporcione un valor para el parámetro **TYPE**, pulse Intro para aceptar el valor predeterminado, o especifique uno de los valores siguientes y luego pulse Intro:

   - 1 para un clúster
   - 2 para un conjunto de réplicas
   - 3 para una instancia autónoma

   De forma predeterminada, el agente supervisa un clúster.
3. Cuando se le solicite que proporcione un valor para el parámetro **PORT**, pulse Intro para aceptar el valor predeterminado, o especifique el número de puerto del direccionador de un clúster de MongoDB o una instancia mongod del conjunto de réplicas MongoDB que se supervisa y a continuación pulse Intro.

   Recuerde: Si no especifica ningún número de puerto, el agente descubre automáticamente el número de puerto del proceso MongoDB adecuado que está activo en la interfaz por omisión. Si no hay ningún proceso de MongoDB activo en la interfaz por omisión, el agente selecciona el número de puerto del proceso MongoDB adecuado que está activo en la interfaz secundaria.
4. Cuando se le solicite que proporcione un valor para el parámetro **HOST**, pulse Intro para aceptar el valor predeterminado, o especifique la dirección IP del sistema host de MongoDB y a continuación pulse Intro.

   Recuerde: Si no especifica ninguna dirección IP, el agente detecta automáticamente la dirección IP del proceso MongoDB adecuado que está activo en la interfaz por omisión. Si no hay ningún proceso de MongoDB activo en la interfaz por omisión, el agente detecta la dirección IP del proceso MongoDB adecuado que está activo en la interfaz secundaria.
5. Cuando se le solicite que proporcione un valor para el parámetro **AUTHENTICATION**, pulse Intro para aceptar el valor predeterminado, o especifique si el agente se está ejecutando en modalidad de autenticación.

   El valor predeterminado es NO, que indica que el agente no se ejecuta en modo de autenticación. Especifique YES para indicar que mongoDB se ejecuta en modo de autenticación.

Recuerde: Cuando la base de datos MongoDB se está ejecutando en modalidad de autenticación, el Agente de MongoDB o cualquier cliente de MongoDB no se puede conectar a la base de datos de MongoDB sin credenciales. Para conectar con la base de datos que se ejecuta en la modalidad de autenticación, especifique YES para el parámetro **AUTHENTICATION**.

Si especifica YES, realice los pasos siguientes:

a) Para el parámetro **Nombre de usuario**, especifique un nombre de usuario para el direccionador o la instancia de mongod. Asegúrese de que se asignan los roles mínimos al usuario. Para obtener información sobre los roles de usuario, consulte Tabla 183 en la página 594.

b) En el parámetro **Contraseña**, especifique la contraseña.

6. Ejecute el mandato siguiente para iniciar el agente:
   dir_instalación/bin/mongodb-agent.sh start *nombre_instancia*

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración de la supervisión de MySQL

El Monitoring Agent for MySQL requiere un nombre de instancia y las credenciales de usuario del servidor MySQL. Puede cambiar los valores de configuración después de crear la primera instancia de agente.

Antes de empezar

- Asegúrese de que se crea un usuario en la base de datos MySQL para ejecutar el agente. El usuario no requiere ningún privilegio específico en la base de datos MySQL que se está supervisando.
- Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de MySQL.

Acerca de esta tarea

Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

El nombre de sistema gestionado incluye el nombre de instancia que especifique, por ejemplo, *nombre_instancia*:*nombre_host*:*pc*, donde *pc* es el código de producto de dos caracteres. El nombre de sistema gestionado puede contener hasta 32 caracteres. El nombre de instancia que especifique puede contener hasta 28 caracteres, excluida la longitud del nombre de host. Por ejemplo, si especifica MySQL2 como nombre de instancia, el nombre de sistema gestionado será MySQL2:nombrehost:SE.

Importante: Si especifica un nombre de instancia largo, el nombre de sistema gestionado queda truncado y el código de agente no se visualiza correctamente.

Configuración del agente en sistemas Windows

Puede utilizar la ventana de IBM Cloud Application Performance Management para configurar el agente en sistemas Windows.

Procedimiento

1. Pulse **Inicio > Todos los programas > Agentes de IBM Monitoring > IBM Performance Management**.
2. En la ventana **IBM Performance Management**, complete estos pasos:
   a) Efectúe una doble pulsación en la plantilla de **Monitoring Agent for MySQL**.
   b) En la ventana **Monitoring Agent for MySQL**, especifique un nombre de instancia y pulse **Aceptar**.
3. En la ventana **Monitoring Agent for MySQL**, complete estos pasos:
   a) En el campo **Dirección IP**, especifique la dirección IP de un servidor MySQL que desea supervisar de forma remota. Si el agente se instala en el servidor a supervisar, retenga el valor predeterminado.
   b) En el campo **Nombre de usuario de JDBC** especifique el nombre de un usuario de servidor MySQL. El valor predeterminado es root.
   c) En el campo **Contraseña de JDBC**, escriba la contraseña de un usuario de JDBC.
   d) En el campo **Confirmar contraseña de JBDC**, escriba de nuevo la contraseña.
   e) En el campo **Archivo Jar JDBC**, pulse **Navegar** y localice el directorio que contiene el archivo Java del conector MySQL, y selecciónelo.
   f) Pulse **Siguiente**.
   g) En el campo **Número de puerto JDBC**, especifique el número de puerto del servidor JDBC.
   El número de puerto predeterminado es 3306.
   h) En la lista **Nivel de rastreo de Java**, seleccione un nivel de rastreo para Java.
   El valor predeterminado es `Error`.
   i) Pulse **Aceptar**.
   La instancia se visualiza en la ventana **IBM Performance Management**.
4. Pulse el botón derecho del ratón en la instancia de **Monitoring Agent for MySQL** y pulse **Iniciar**.

   Recuerde: Para configurar el agente de nuevo, complete estos pasos en la ventana de **IBM Performance Management**:

   a. Detenga la instancia de agente que desea configurar.
   b. Pulse el botón derecho del ratón en la instancia de **Monitoring Agent for MySQL** y pulse **Reconfigurar**.
   c. Repita los pasos 3 y 4.

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del agente en sistemas Linux

Ejecute el script de configuración para configurar el agente en sistemas Linux.

Procedimiento

1. Ejecute el mandato siguiente:

   ```
   dir_instalación/bin/mysql-agent.sh
   config nombre_instancia
   ```

   Donde *nombre_instancia* es el nombre que desea dar a la instancia y *dir_instalación* es el directorio de instalación del Agente de MySQL.
2. Cuando se le solicite que especifique un valor para los parámetros siguientes, presione la tecla Intro para aceptar el valor predeterminado o especifique otro valor y presione la tecla Intro.
   - Dirección IP

- Nombre de usuario de JDBC
- Contraseña de JDBC
- Vuelva a escribir: contraseña de JDBC
- Archivo .jar de JDBC
- Número de puerto de JDBC (el número de puerto predeterminado es 3306.)
- Nivel de rastreo Java (el valor predeterminado es `Error`.)

Para obtener más información sobre los parámetros de configuración, consulte "Configuración del agente mediante el archivo de respuestas silencioso" en la página 601.

3. Ejecute el mandato siguiente para iniciar el agente.

```
dir_instalación/bin/mysql-agent.sh start nombre_instancia
```

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del agente mediante el archivo de respuestas silencioso

Utilice el archivo de respuestas silencioso para configurar el agente sin responder a las solicitudes cuando ejecuta el script de configuración. Puede utilizar el archivo de respuestas silencioso para configurar el agente en sistemas Windows y Linux.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración. Puede editar los valores de estos parámetros en el archivo de respuestas y ejecutar el script de configuración para crear una instancia de agente y actualizar los valores de configuración.

Procedimiento

1. En un editor de texto, abra el archivo de respuestas que está disponible en la siguiente vía de acceso:

   Linux *dir_instalación*`/samples/mysql_silent_config.txt`

   Windows *dir_instalación*`\samples\mysql_silent_config.txt`

   Donde *dir_instalación* es el directorio de instalación del Agente de MySQL.
2. En el archivo de respuestas, especifique un valor para los parámetros siguientes:
   - Para el parámetro **`Nombre de servidor`** especifique la dirección IP de un servidor MySQL que desea supervisar de forma remota. De lo contrario, retenga el valor predeterminado como `localhost`.
   - Para el parámetro **`Nombre de usuario de JDBC`**, retenga el valor de nombre de usuario predeterminado de `root` o especifique el nombre de un usuario con privilegios para ver las tablas INFORMATION_SCHEMA.
   - Para el parámetro **`Contraseña de JDBC`**, especifique una contraseña de usuario de JDBC.
   - Para el parámetro **`Archivo .jar de JDBC`**, retenga la vía de acceso predeterminada si esta vía de acceso del conector MySQL para el archivo .jar de Java es correcta. De lo contrario, entre la vía de acceso correcta. El conector está disponible en la vía de acceso predeterminada siguiente:

     Linux `/usr/share/java/mysql-connector-java.jar`

     Windows `C:\Program Files (x86)\MySQL\Connector J 5.1.26\mysql-connector-java-5.1.26-bin.jar`
   - Para el **`Número de puerto de JDBC`**, retenga el número de puerto predeterminado de 3306 o especifique otro número de puerto.

- Para el parámetro **Nivel de rastreo de Java**, retenga el valor predeterminado de `Error` o un nivel distinto de acuerdo con las instrucciones del soporte de IBM.

3. Guarde y cierre el archivo de respuestas y ejecute el mandato siguiente para actualizar los valores de configuración del agente:

   Linux *dir_instalación*`/bin/mysql-agent.sh config` *nombre_instancia* *dir_instalación*`/samples/mysql_silent_config.txt`

   Windows *dir_instalación*`\BIN\mysql-agent.bat config` *nombre_instancia* *dir_instalación*`\samples\mysql_silent_config.txt`

   Donde *nombre_instancia* es el nombre que desea dar a la instancia y *dir_instalación* es el directorio de instalación del Agente de MySQL.

   Importante: Asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silenciosas. De lo contrario, no habrá datos de agente mostrados en los paneles de instrumentos.

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración de la supervisión de NetApp Storage

El Monitoring Agent for NetApp Storage supervisa los sistemas de almacenamiento NetApp mediante NetApp OnCommand Unified Manager, OnCommand API Services y OnCommand Performance Manager.

Antes de empezar

- Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de NetApp Storage.
- Asegúrese de que los siguientes componentes están instalados en la máquina:
  - OnCommand Unified Manager
  - OnCommand Performance Manager
  - OnCommand API Services

  Para obtener más información sobre la instalación de estos componentes, consulte la documentación de NetApp.
- Asegúrese de que las versiones de OnCommand API Services, OnCommand Unified Manager y OnCommand Performance Manager sean compatibles. Por ejemplo, para configurar OnCommand API Services V1.0, empareje OnCommand Unified Manager V6.2, V6.1 o V6.0 con OnCommand Performance Manager V1.1. Para conocer las versiones de producto compatibles, consulte la Herramienta de matriz de interoperatividad.
- Asegúrese de que el usuario que se conecta a OnCommand Unified Manager tiene el privilegio GlobalRead sobre el sistema de almacenamiento de NetApp que se está supervisando. Utilice un ID de usuario existente con este privilegio o cree un ID de usuario nuevo. Para obtener información acerca de la creación del ID de usuario en el sistema de almacenamiento de NetApp, consulte la documentación de NetApp .
- Asegúrese de que el usuario utilizado para conectarse a nCommand API Services sea un administrador o supervisor. Estos tipos de usuario tiene permisos predeterminados para ejecutar la API REST.
- Descargue el archivo JAR del SDK de NetApp Manageability (`manageontap.jar`) del sitio web de NetApp e instálelo en el directorio `lib` del agente de supervisión siguiendo los pasos indicados en la sección "Descarga e instalación del archivo JAR del SDK de NetApp Manageability" en la página 603.

Acerca de esta tarea

El Agente de NetApp Storage es un agente de varias instancias. Deberá crear la primera instancia e iniciar el agente manualmente.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

- Para configurar el agente en sistemas Windows, puede utilizar la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
- Para configurar el agente en sistemas Linux, puede ejecutar el script y responder a las solicitudes, o utilizar el archivo de respuestas silencioso.

Descarga e instalación del archivo JAR del SDK de NetApp Manageability

El Agente de NetApp Storage requiere el archivo JAR del SDK de NetApp Manageability para comunicarse con un servidor NetApp OCUM.

Acerca de esta tarea

Tras instalar el Agente de NetApp Storage, descargue el archivo JAR del SDK de NetApp Manageability (`manageontap.jar`) del sitio web de NetApp e instálelo en el directorio `lib` del agente de supervisión.

Procedimiento

1. Descargue el archivo comprimido que contiene el archivo JAR del siguiente sitio web: http://communities.netapp.com/docs/DOC-1152.
2. Extraiga el archivo comprimido y copie el archivo `manageontap.jar` en las ubicaciones siguientes:
   - Para sistemas Windows de 32 bits, copie el archivo en *dir_instalación*`/tmaitm6`
   - Para sistemas Windows de 64 bits, copie el archivo en *dir_instalación*`/tmaitm6_x64`
   - Para sistemas Linux de 32 bits, copie el archivo en *dir_instalación*`/li6263/nu/lib`
   - Para sistemas Linux de 64 bits x86-64, copie el archivo en *dir_instalación*`/lx8266/nu/lib`
   - Para sistemas zLinux de 64 bits, copie el archivo en *dir_instalación*`/ls3266/nu/lib`

Qué hacer a continuación

Complete la configuración del agente.

Configuración del agente en sistemas Windows

Puede configurar el agente en sistemas operativos Windows mediante la ventana **IBM Performance Management**. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Acerca de esta tarea

El Agente de NetApp Storage proporciona valores predeterminados para algunos parámetros. Puede especificar diferentes valores para estos parámetros.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Monitoring Agent for NetApp Storage** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar el agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar el agente de nuevo, pulse **Reconfigurar**.

3. En la ventana Monitoring Agent for NetApp Storage, realice los pasos siguientes:
   a) Escriba un nombre exclusivo para la instancia del Agente de NetApp Storage y pulse **Aceptar**.
   b) En la pestaña **Proveedor de datos**, especifique valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.
   c) En la pestaña **OnCommand Unified Manager**, especifique valores para los parámetros de configuración y pulse **Siguiente**.
   d) En la pestaña **OnCommand API Service**, especifique valores para los parámetros de configuración y pulse **Aceptar**.

   Para obtener información sobre los parámetros de configuración de cada pestaña de la ventana Monitoring Agent for NetApp Storage, consulte los temas siguientes:

   - "Parámetros de configuración del proveedor de datos" en la página 606
   - "Parámetros de configuración de OnCommand Unified Manager" en la página 607
   - "Parámetros de configuración de OnCommand API Service" en la página 608
4. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Monitoring Agent for NetApp Storage** y luego pulse **Iniciar**.

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

- Para configurar el Agente de NetApp Storage en modalidad silenciosa, realice los pasos siguientes:
  a) En un editor de texto, abra el archivo `netapp_storage_silent_config.txt` que está disponible en la siguiente vía de acceso:
     – Linux *dir_instalación*`/samples/netapp_storage_silent_config.txt`

       Ejemplo: `/opt/ibm/apm/agent/samples/netapp_storage_silent_config.txt`
     – Windows *dir_instalación*`\samples\netapp_storage_silent_config.txt`

       Ejemplo: `C:\IBM\APM\samples\netapp_storage_silent_config.txt`
  b) En el archivo `netapp_storage_silent_config.txt`, especifique valores para todos los parámetros obligatorios. También puede modificar los valores predeterminados de otros parámetros.

     Para obtener información sobre los parámetros de configuración, consulte los siguientes temas:

- "Parámetros de configuración del proveedor de datos" en la página 606
- "Parámetros de configuración de OnCommand Unified Manager" en la página 607
- "Parámetros de configuración de OnCommand API Service" en la página 608

c) Guarde y cierre el archivo `netapp_storage_silent_config.txt` y ejecute el mandato siguiente:

- Linux *dir_instalación*`/bin/netapp_storage-agent.sh config` *nombre_instancia dir_instalación*`/samples/netapp_storage_silent_config.txt`

  Ejemplo: **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh config nombre_instancia /opt/ibm/apm/agent/samples/netapp_storage_silent_config.txt**

- Windows *dir_instalación*`\bin\netapp_storage-agent.bat config` *nombre_instancia dir_instalación*`\samples\netapp_storage_silent_config.txt`

  Ejemplo: **C:\IBM\APM\bin\netapp_storage-agent.bat config nombre_instancia C:\IBM\APM\samples\netapp_storage_silent_config.txt**

  Donde

  nombre_instancia
  Nombre que desea dar a la instancia.

  dir_instalación
  Vía de acceso donde está instalado el agente.

Importante: asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

d) Ejecute el mandato siguiente para iniciar el agente:

- Linux *dir_instalación*`/bin/netapp_storage-agent.sh start` *nombre_instancia*

  Ejemplo: **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh start nombre_instancia**

- Windows *dir_instalación*`\bin\netapp_storage-agent.bat start` *nombre_instancia*

  Ejemplo: **C:\IBM\APM\bin\netapp_storage-agent.bat start nombre_instancia**

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente respondiendo a solicitudes

Para configurar el agente en sistemas Linux, debe ejecutar el script y responder a las solicitudes.

Procedimiento

1. En la línea de mandatos, entre el siguiente mandato:

   dir_instalación`/bin/netapp_storage-agent.sh config` *nombre_instancia*

   Ejemplo: **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh config nombre_instancia**

Donde

nombre_instancia
Nombre que desea dar a la instancia.

dir_instalación
Vía de acceso donde está instalado el agente.

2. Responda a las solicitudes haciendo referencia a los temas siguientes:
   - "Parámetros de configuración del proveedor de datos" en la página 606
   - "Parámetros de configuración de OnCommand Unified Manager" en la página 607
   - "Parámetros de configuración de OnCommand API Service" en la página 608
3. Ejecute el mandato siguiente para iniciar el agente:

   dir_instalación/bin/netapp_storage-agent.sh start *nombre_instancia*

   Ejemplo: **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh start nombre_instancia**

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Parámetros de configuración del proveedor de datos

Al configurar el Agente de NetApp Storage, puede cambiar los valores predeterminados de los parámetros del proveedor de datos, por ejemplo el número máximo de archivos de registro del proveedor de datos, el tamaño máximo del archivo de registro y el nivel de detalle que se incluye en el archivo de registro.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del proveedor de datos.

Tabla 184. Nombres y descripciones de los parámetros de configuración del proveedor de datos

Nombre de parámetro	Descripción	Campo obligatorio
Nombre de instancia (**KNU_INSTANCE_NAME**)	El nombre de la instancia. **Restricción:** El campo Nombre de instancia muestra el nombre de la instancia que especifica al configurar el agente por primera vez. Al volver a configurar el agente, no puede cambiar el nombre de instancia del agente.	Sí
Número máximo de archivos de registro del proveedor de datos (**KNU_LOG_FILE_MAX_COUNT**)	El número máximo de archivos de registro que el proveedor de datos crea antes de grabar encima de los archivos de registro anteriores. El valor predeterminado es 10.	Sí
Tamaño máximo en KB de cada archivo de registro del proveedor de datos (**KNU_LOG_FILE_MAX_SIZE**)	El tamaño máximo en KB que debe alcanzar un archivo de registro del proveedor de datos antes de que el proveedor de datos cree un archivo de registro nuevo. El valor predeterminado es 5190 KB.	Sí

Tabla 184. Nombres y descripciones de los parámetros de configuración del proveedor de datos (continuación)		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Nivel de detalle en el archivo de registro del proveedor de datos (**KNU_LOG_LEVEL**)	El nivel de detalle que puede incluirse en el archivo de registro que crea el proveedor de datos. El valor predeterminado es 4 (Info). Los valores siguientes son válidos: • 1 (Desactivado): no se registra ningún mensaje. • 2 (Grave): sólo se registran los errores. • 3 (Aviso): todos los errores y mensajes que se registran en el nivel Grave y los errores potenciales que pueden provocar un comportamiento indeseable. • 4 (Info): todos los errores y mensajes que se registran en el nivel Aviso y los mensajes informativos de alto nivel que describen el estado del proveedor de datos cuando se procesa. • 5 (Bueno): todos los errores y mensajes que se registran en el nivel Info y los mensajes informativos de bajo nivel que describen el estado del proveedor de datos cuando se procesa. • 6 (Mejor): todos los errores y mensajes que se registran en el nivel Bueno y los mensajes informativos muy detallados, como por ejemplo la información de perfilado de rendimiento y datos de depuración. Si selecciona esta opción, el rendimiento del agente de supervisión puede verse perjudicado. Este valor está concebido para utilizarlo como herramienta para la determinación de problemas en colaboración con el personal de soporte de IBM. • 7 (El mejor): todos los errores y mensajes que se registran en el nivel Bueno y los mensajes informativos más detallados que incluyen datos y mensajes de programación de bajo nivel. Si selecciona esta opción, el rendimiento del agente de supervisión puede verse perjudicado. Este valor está concebido para utilizarlo como herramienta para la determinación de problemas en colaboración con el personal de soporte de IBM. • 8 (Todos): se registran todos los mensajes.	Sí

Parámetros de configuración de OnCommand Unified Manager

Al configurar el Agente de NetApp Storage, puede cambiar los valores predeterminados de los parámetros de OCUM (OnCommand Unified Manager), como la dirección IP del servidor OCUM, el nombre de usuario y la contraseña.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del origen de datos.

Tabla 185. Nombres y descripciones de los parámetros de configuración de OnCommand Unified Manager		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Servidor (**KNU_DATASOURCE_HOST_ADDRESS**)	El nombre de host o dirección IP del servidor OCUM de NetApp que debe supervisarse.	Sí

Tabla 185. Nombres y descripciones de los parámetros de configuración de OnCommand Unified Manager (continuación)		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Usuario (**KNU_DATASOURCE_USERNAME**)	Un nombre de usuario del servidor OCUM de NetApp con privilegios suficientes para recopilar datos. El valor predeterminado es admin.	Sí
Contraseña (**KNU_DATASOURCE_PASSWORD**)	La contraseña del usuario que ha especificado en el parámetro **Usuario**.	Sí
Confirmar contraseña	La misma contraseña que ha especificado en el parámetro **Especificar contraseña**.	Sí
Protocolo (**KNU_DATASOURCE_PROTOCOL**)	El protocolo que debe utilizarse para comunicarse con el servidor OCUM de NetApp. El valor predeterminado es HTTPS.	Sí

Parámetros de configuración de OnCommand API Service

Al configurar el Agente de NetApp Storage, puede cambiar los valores predeterminados de los parámetros de OnCommand API Service, como la dirección de host, el nombre de usuario y la contraseña.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del origen de datos.

Tabla 186. Nombres y descripciones de los parámetros de configuración de OnCommand API Service		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Dirección de host (**KNU_API_SERVICES_HOST_ADDRESS**)	Nombre de host o dirección IP del servicio de OnCommand API.	Sí
Usuario (**KNU_API_SERVICES_USERNAME**)	Un nombre de usuario con privilegios suficientes para conectarse al servicio OnCommand API. El valor predeterminado es admin.	Sí
Contraseña (**KNU_API_SERVICES_PASSWORD**)	La contraseña del usuario que ha especificado en el parámetro **Usuario**.	
Confirmar contraseña	La misma contraseña que ha especificado en el parámetro **Especificar contraseña**.	Sí

Configuración de la supervisión de Node.js

Puede utilizar el agente de Node.js o el recopilador de datos de Node.js autónomo para supervisar las aplicaciones Node.js. Si desea utilizar un proceso de instalación más simple y la función de rastreo de transacciones, utilice el recopilador de datos de Node.js.

Antes de empezar

- Las instrucciones siguientes corresponden al release más reciente de este agente y recopilador de datos. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte “Historial de cambios” en la página 52.

- Asegúrese de que se cumplen los requisitos del sistema para el Agente de Node.js o Recopilador de datos de Node.js en su entorno.
  - Para obtener información actualizada sobre los requisitos del sistema del Agente de Node.js, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Node.js.
  - Para obtener información actualizada sobre los requisitos del sistema del Recopilador de datos de Node.js, consulte el Software Product Compatibility Reports (SPCR) para el Recopilador de datos de Node.js.

Acerca de esta tarea

El procedimiento siguiente es una hoja de ruta para configurar el Monitoring Agent for Node.js y el recopilador de datos de Node.js autónomo que incluye pasos obligatorios y opcionales.

- Para supervisar aplicaciones locales, puede configurar el Recopilador de datos de Node.js autónomo o el Agente de Node.js. Si desea habilitar el rastreo de transacciones para sus aplicaciones Node.js, configure el recopilador de datos autónomo.
- Para supervisar las aplicaciones de IBM Cloud(anteriormente Bluemix) o Kubernetes, configure el Recopilador de datos de Node.js autónomo.

Siga estos pasos según sus necesidades.

Procedimiento

- Configure el Agente de Node.js para supervisar las aplicaciones locales.
  a) Añada un recopilador de datos de agente a las aplicaciones Node.js para que el agente funcione adecuadamente. Consulte “Configuración del Agente de Node.js” en la página 609.
  b) Opcional: Para cambiar el comportamiento de supervisión del agente, consulte Configuración del recopilador de datos del Agente de Node.js.
  c) Opcional: Para configurar la recopilación y visualización de datos de diagnóstico, consulte Configuración del recopilador de datos de diagnóstico.
- Configure el Recopilador de datos de Node.js autónomo para supervisar aplicaciones IBM Cloud.
  a) Para configurar el Recopilador de datos de Node.js autónomo, consulte “Configuración del Recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud (anteriormente Bluemix)” en la página 615.
  b) Para cambiar el comportamiento del Recopilador de datos de Node.js autónomo, consulte “Personalización del recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud” en la página 617.
- Configure el Recopilador de datos de Node.js autónomo para supervisar aplicaciones locales.
  a) Para configurar el Recopilador de datos de Node.js autónomo, consulte “Configuración del Recopilador de datos de Node.js autónomo para aplicaciones locales” en la página 621.
  b) Para cambiar el comportamiento del Recopilador de datos de Node.js autónomo, consulte “Personalización del Recopilador de datos de Node.js para aplicaciones locales” en la página 623.
- Configure el Recopilador de datos de Node.js autónomo para supervisar las aplicaciones en Kubernetes.
  a) Para configurar el Recopilador de datos de Node.js autónomo, consulte “Configuración del Recopilador de datos de Node.js autónomo para aplicaciones Kubernetes” en la página 627.
  b) Para cambiar el comportamiento del Recopilador de datos de Node.js autónomo, consulte “Personalización del recopilador de datos de Node.js autónomo para aplicaciones Kubernetes” en la página 628.

Configuración del Agente de Node.js

Debe añadir un recopilador de datos de agente a la aplicación Node.js y reiniciarlo para que el agente pueda empezar a supervisar la aplicación.

Antes de empezar

Antes de reconfigurar los valores del agente dentro de la misma versión, siga estos pasos para borrar los archivos del recopilador de datos creados por la configuración anterior:

1. Acceda al directorio *dir_instalación*/lx8266/nj/bin.
2. Ejecute el mandato ./uninstall.sh para eliminar los archivos del recopilador de datos existentes.

Acerca de esta tarea

El agente Node.js es un agente de instancia única. Registra subnodos para cada aplicación Node.js supervisada. El subnodo se encuentra en la estructura siguiente:

NJ:nombrehost_puerto:NJA

Consejo: si una aplicación Node.js está a la escucha en varios números de puerto, se utilizará el número de puerto más bajo.

Debe añadir un recopilador de datos de agente a la aplicación Node.js y reiniciar la aplicación para que el agente pueda empezar a supervisar la aplicación. Los recopiladores de datos de agente recopilan datos que se reenvían al agente de Node.js. Actualmente, se suministran los siguientes recopiladores de datos de agente:

- El recopilador de datos de recurso recopila datos de supervisión de recursos de las aplicaciones Node.js.
- El recopilador de datos de diagnóstico recopila datos de diagnóstico y datos de supervisión de recursos de las aplicaciones Node.js.
- El recopilador de datos de rastreo de método recopila rastreos de método, datos de diagnóstico y datos de supervisión de recursos de las aplicaciones Node.js.

Procedimiento

1. Asegúrese de que el ID de usuario que se utiliza para ejecutar el servidor de aplicaciones tiene permiso completo en el directorio dir_instalación del agente.
2. Vaya al directorio *dir_instalación*/bin y ejecute el mandato siguiente:

```
./nodejs-agent.sh config
```

3. Siga las solicitudes para especificar valores para las siguientes opciones de configuración:

   KNJ_NODEJS_RUNTIME_BIN_LOCATION
   El directorio a la carpeta bin del tiempo de ejecución de Node.js. El directorio predeterminado es /usr/local/bin.

   KNJ_NPM_RUNTIME_BIN_LOCATION
   El directorio a la carpeta bin del mandato **npm**. El directorio predeterminado es /usr/local/bin.

   KNJ_NPM_LIB_LOCATION
   El directorio a la carpeta lib del directorio de instalación global del paquete npm. El directorio predeterminado es /usr/local/lib. Por ejemplo, si instala el paquete npm ejecutando el mandato npm install -g, el paquete se instala en /*inicio_nodejs*/lib/node_modules y **KNJ_NPM_LIB_LOCATION** es /*inicio_nodejs*/lib.

   CP_PORT
   El puerto que el agente utiliza para escuchar los datos de los clientes de socket. El valor 0 indica que se utilizará un puerto efímero. El valor predeterminado es 63336.

   Nota: no utilice un número de puerto que ya se utilice en el sistema. Para comprobar si el puerto ya se está utilizando, ejecute el mandato netstat -apn | grep *número_puerto*.

4. Inicie el agente ejecutando el mandato siguiente:

```
./nodejs-agent.sh start
```

5. Compruebe que el Agente de Node.js se ha iniciado correctamente. Si el agente se ha iniciado correctamente, se generará la carpeta *KNJ_NPM_LIB_LOCATION*/node_modules/ibmapm.
6. En función de la oferta de que disponga y sus requisitos, inserte una de las entradas siguientes en el archivo .js de la aplicación Node.js para configurar los recopiladores de datos de agente:

   Nota: sólo puede añadirse una entrada a la aplicación Node.js para habilitar las prestaciones de recopilador de datos de agente. Además, si habilita prestaciones que no estén incluidas en la oferta, puede producirse una sobrecarga innecesaria, disminuyendo la eficiencia de ejecución de la aplicación.

   - Si sólo dispone de prestaciones de supervisión de recursos, puede añadir el recopilador de datos de recurso. Para añadirlo, inserte la línea siguiente al principio del archivo de aplicación Node.js:

     ```
     require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm');
     ```

     Si el valor de **KNJ_NPM_LIB_LOCATION** en el entorno es /usr/local/lib, la línea será

     ```
     require('/usr/local/lib/node_modules/ibmapm');
     ```

   - Si dispone de prestaciones de diagnóstico además de las prestaciones de supervisión a nivel de recurso, puede elegir añadir uno de los siguientes recopiladores de datos de agente:
     - Para añadir el recopilador de datos de rastreo de método, inserte la línea siguiente al principio del archivo de aplicación Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/methodtrace.js');
       ```

     - Para añadir el recopilador de datos de diagnóstico, inserte la línea siguiente al principio del archivo de aplicación Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/deepdive.js');
       ```

     - Para añadir el recopilador de datos de supervisión de recursos, inserte la línea siguiente al principio del archivo de aplicación Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm');
       ```

     Para garantizar el mejor rendimiento, añada el recopilador de datos de rastreo de método sólo a efectos de depuración.

   Nota: El código de los plug-ins cambia a partir de Cloud APM Marzo de 2017. Si actualiza el agente desde versiones anteriores, debe actualizar el código de los recopiladores de datos existentes en las aplicaciones para que la capacidad de supervisión funcione correctamente.
7. Reinicie la aplicación Node.js para inhabilitar los plug-in de recopilador de datos de agente.

Resultados
Ha configurado satisfactoriamente el Agente de Node.js.

Qué hacer a continuación

- Ahora, puede verificar que los datos del Agente de Node.js se visualizan en la consola de Cloud APM. Si desea instrucciones sobre cómo iniciar la consola de Cloud APM, consulte la sección Inicio de la consola de Cloud APM. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte Gestión de aplicaciones.

  Importante: para añadir la aplicación a la Consola de Cloud APM, elija **Node.js** en el editor de aplicaciones.
- Puede cambiar el comportamiento de tiempo de ejecución de los recopiladores de datos de agente de Node.js. Para obtener más información, consulte la sección Configuración del recopilador de datos del agente de Node.js.

- Puede habilitar la recopilación de datos de diagnóstico y visualizarla configurando el recopilador de datos de diagnóstico. Para obtener más información, consulte la sección Configuración del recopilador de datos de diagnóstico.

Configuración del recopilador de datos del Agente de Node.js
Puede cambiar el comportamiento de cada recopilador de datos de agente de Node.js cambiando su configuración de tiempo de ejecución en su archivo de configuración.

Archivo de configuración de tiempo de ejecución

El código del recopilador de datos de Node.js está en el directorio siguiente:

KNJ_NPM_LIB_LOCATION/node_modules/ibmapm

donde *KNJ_NPM_LIB_LOCATION* es el directorio a la carpeta lib del directorio de instalación global del paquete npm. El directorio predeterminado es /usr/local/lib.

También hay un archivo de configuración para cada recopilador de datos de agente en la misma carpeta. El recopilador de datos de agente lee el archivo de configuración cada minuto.

Consejo: el archivo de configuración de tiempo de ejecución se nombra con el formato siguiente:

plugin_*número de puerto de aplicación*_conf.json

Cuando cambia el contenido del archivo de configuración, cambia el comportamiento del recopilador de datos de agente asociado. En el archivo de configuración puede cambiar dos tipos de información:

- Reglas de filtrado de URL
- Parámetros de registro del recopilador de datos de agente

Reglas de filtrado de URL

Puede cambiar las reglas de filtrado de URL en el archivo de configuración de tiempo de ejecución. Se utilizan expresiones regulares para correlacionar el nombre de vía de acceso del URL con un nombre de vía de acceso personalizado del usuario. Puede correlacionar el URL con un nombre de vía de acceso personalizado para satisfacer los requisitos siguientes:

- Agregar URLs con vías de acceso similares. Por ejemplo, si tiene las siguientes vías de acceso de URL:

```
/demo/poll/1
/demo/poll/2
/demo/poll/3
...
```

  En el servidor web, probablemente se da servicio a las solicitudes para estas vías de acceso mediante una rutina común, por lo que puede agregar las vías de acceso a un solo tipo de URL mediante un filtro utilizando el filtro del ejemplo siguiente.

```
"filters":
[
    {
        "pattern": "/demo/poll/.+",
        "to": "/demo/poll/"
    }
```

  Este filtro da como resultado que todas las solicitudes de las vías de acceso de URL como "/demo/poll/xxx" se correlacionen con un tipo de vía de acceso de URL de "/demo/poll". A continuación, se hace un promedio del tiempo de respuesta de todas las solicitudes para las vías de acceso de URL de este tipo a un solo valor. La agregación de esta manera puede ayudar a hacer un uso más eficiente de los recursos disponibles.
- Ignorar las vías de acceso de URL a archivos estáticos o filtrar determinados tipos de solicitudes. Por ejemplo, si una página web incluye imágenes que generan solicitudes de descarga de servidor individuales, quizá no le interese ver los tiempos de respuesta para estos tipos de solicitudes.

Para filtrar un tipo de solicitud, establezca el valor "to" en vacío como en el formato del ejemplo siguiente:

```
"filters":
[
    {
        "pattern": "GET /css/.+\\.css$",
        "to": ""
    }
```

Este filtro hace que las solicitudes obtengan un archivo `.css` que debe ignorarse. Como resultado, puede utilizar los recursos disponibles de forma más eficiente en las solicitudes que necesite supervisar.

En el archivo de configuración, las reglas de filtro de URL se especifican en una matriz JSON denominada `filters`:

```
"filters":
[
    {
        "pattern": ".+\\.png$",
        "to": ""
    },
    {
        "pattern": ".+\\.jpg$",
        "to": ""
    },
    {
        "pattern": "GET /js/.+\\.js$",
        "to": ""
    },
    {
        "pattern": "GET /css/.+\\.css$",
        "to": ""
    }
]
```

Cada miembro de la matriz es una regla de filtrado. Cuando el recopilador de datos de agente recibe una solicitud HTTP, extrae el nombre de vía de acceso de URL de la solicitud y lo compara con cada `"pattern"` (patrón). Si el nombre de vía de acceso no coincide con un `"pattern"`, el nombre de vía de acceso de URL original se mantiene y se utiliza para las mediciones.

Parámetro de registro del recopilador de datos de agente

Puede cambiar los comportamientos de registro modificando el parámetro en el archivo de configuración `config.properties` del directorio *KNJ_NPM_LIB_LOCATION*`/node_modules/ibmapm/etc`. Se proporciona el parámetro de registro siguiente, que puede cambiar:

El nivel de rastreo

La entrada del archivo de configuración del nivel de rastreo es `KNJ_LOG_LEVEL=info`, lo que significa que la información de resumen sobre las acciones se imprime en el registro. Puede establecer el nivel de registro cambiando el valor de `KNJ_LOG_LEVEL`. El valor predeterminado es `info` y el registro se imprime en la salida estándar.

Se da soporte a los cinco valores de nivel de registro siguientes;

off
Los registros no se imprimen.

error
Solo se registra información si se da una condición de error.

info
Se registra información cuando el recopilador de datos del Agente de Node.js se ejecuta normalmente. También se registran los datos de supervisión en bruto enviados al agente.

debug
Se anota información de depuración, información y error útil en el registro, por ejemplo, datos recopilados, datos que se envían al servidor y la respuesta del servidor.

all
Se anota toda la información en el registro.

Configuración del recopilador de datos de diagnóstico del Agente de Node.js
El soporte para la recopilación de datos de diagnóstico está inhabilitado de forma predeterminada. Si dispone de prestaciones de diagnóstico, debe establecer y ajustar la recopilación de datos para aplicaciones Node.js específicas.

Procedimiento

- Para modificar los valores del recopilador de datos de una aplicación específica en ejecución:
  1. Vaya al directorio *KNJ_NPM_LIB_LOCATION*/node_modules/ibmapm y abra el archivo plugin_*puerto*_conf.json en un editor de textos.

     Consejo: Para obtener información sobre *KNJ_NPM_LIB_LOCATION*, consulte la descripción de parámetro de "KNJ_NPM_LIB_LOCATION" en la página 610
  2. Utilice la tabla siguiente para obtener información acerca de la modificación de valores del recopilador de datos:

Tabla 187. Valores del recopilador de datos

Categoría de datos de diagnóstico	Descripción	Propiedad	Acción
Delta de tiempo mínimo para informes de seguimiento de la pila	Especifica el umbral de tiempo de respuesta para recopilar el seguimiento de pila de una solicitud o una llamada de método. Si el tiempo de respuesta de una solicitud o llamada de método supera este valor, el recopilador de datos recopila su seguimiento de pila.	minClockStack	Establézcalo en un valor en milisegundos
Delta de tiempo mínimo para solicitudes de informe	Especifica el umbral de tiempo de respuesta para recopilar el rastreo de método de una instancia de solicitud. Si el tiempo de respuesta de una instancia de solicitud supera este valor, el recopilador de datos recopila su rastreo de método.	minClockTrace	Establézcalo en un valor en milisegundos

Tabla 187. Valores del recopilador de datos (continuación)

Categoría de datos de diagnóstico	Descripción	Propiedad	Acción
Número máximo de sucesos por archivo	Especifica el número máximo de sucesos que deben registrarse en un archivo `.jso`. El archivo `.jso` registra los datos de diagnóstico de estos sucesos.	`eventsPerFile`	Establézcalo en un valor de número máximo de sucesos
Cantidad máxima de tiempo para el informe en un archivo	Especifica la cantidad máxima de tiempo para que el archivo `.jso` registre datos de diagnóstico.	`fileCommitTime`	Establézcalo en el tiempo máximo en segundos
Número máximo de archivos a conservar antes de que se supriman los más antiguos	Especifica el número máximo de archivos `.jso` a conservar antes de que se supriman los más antiguos.	`maxFiles`	Establézcalo en el número máximo de archivos
Período de muestreo de solicitud	Especifica el periodo de muestreo de las solicitudes.	`sampling`	Establézcalo en el período de muestro deseado. El valor predeterminado es `10`. Un valor de `10` significa que el agente recopila una de cada 10 solicitudes.

- Opcional: Establezca la variable de entorno *SECURITY_OFF* si desea que el recopilador de datos de diagnóstico recopile información confidencial del usuario como por ejemplo cookies, contextos de solicitud HTTP y contexto de solicitudes de base de datos. Esta información no se recopila de forma predeterminada.

  Tenga cuidado al establecer esta variable porque puede provocar una fuga de información.

  Linux Por ejemplo, para establecer esta variable de entorno, emita el mandato siguiente:

  ```
  export SECURITY_OFF=true
  ```

Resultados

La configuración del recopilador de datos de diagnóstico se ha cambiado para la aplicación en ejecución que ha especificado o para todas las aplicaciones.

Configuración del Recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud (anteriormente Bluemix)

Para recopilar información sobre aplicaciones Node.js en IBM Cloud, debe configurar el Recopilador de datos de Node.js autónomo.

Antes de empezar

1. Asegúrese de que la aplicación Node.js puede ejecutarse correctamente de forma local. El Recopilador de datos de Node.js autónomo puede supervisar Node.js V8.0.0 y fixpacks futuros, V10.0.0 y fixpacks futuros y V12.0.0 y fixpacks futuros.
2. Descargue el paquete de recopilador de datos del sitio web de IBM Marketplace.Para obtener instrucciones detalladas, consulte “Descarga de los agentes y recopiladores de datos” en la página 107.

Procedimiento

1. Extraiga los archivos del paquete del recopilador de datos. El paquete `nodejs_datacollector_8.1.4.0.6.tgz` está incluido en el directorio extraído.
2. Extraiga el archivo `nodejs_datacollector_8.1.4.0.6.tgz`, por ejemplo, ejecutando el mandato siguiente:

   ```
   tar -zxf nodejs_datacollector_8.1.4.0.6.tgz
   ```

3. Extraiga el archivo `ibmapm.tgz` en la carpeta `nodejs_dc` ejecutando el mandato siguiente:

   ```
   tar -zxf nodejs_dc/ibmapm.tgz
   ```

   Obtendrá una carpeta `ibmapm`.
4. Copie la carpeta `ibmapm` que se ha extraído del paquete recopilador de datos en el directorio de inicio de la aplicación, por ejemplo, ejecutando el mandato siguiente:

   ```
   cp –r directorio_para_carpeta_ibmapm  directorio_inicio_aplicación_Node.js
   ```

   Consejo: el directorio de inicio de la aplicación Node.js está determinado por el mandato utilizado para iniciar la aplicación Node.js y por el directorio que contiene el archivo principal. Si utiliza el mandato **node app.js** para iniciar la aplicación Node.js y el archivo principal `app.js` se encuentra en el directorio `/root/nodejs_app`, el directorio de inicio de la aplicación es `/root/nodejs_app`.
5. En el archivo `package.json` de la aplicación Node.js, añada la línea siguiente a la sección de dependencias:

   ```
   “ibmapm": "./ibmapm"
   ```

   Recuerde: no olvide especificar la coma al final de cada línea del archivo excepto la última, y mantener el formato correcto del archivo `package.json`.

   Ejemplo:

   ```
   "dependencies": {
      "ibmapm": "./ibmapm",
      "cors": "^2.5.2",
      "helmet": "^1.3.0",
      "loopback": "^2.22.0",
      "loopback-boot": "^2.6.5",
      "loopback-datasource-juggler": "^2.39.0",
      "serve-favicon": "^2.0.1",
      "strong-error-handler": "^1.0.1"
    }
   ```

6. Añada la línea siguiente al principio del archivo principal de la aplicación Node.js:

   ```
   require('ibmapm');
   ```

   Si inicia la aplicación ejecutando el mandato **app.js**, `app.js` es el archivo principal de la aplicación.
7. En el directorio que contiene el archivo `manifest.yml` de la aplicación Node.js, inicie la sesión en IBM Cloud y ejecute el mandato siguiente:

   ```
   cf push
   ```

Consejo: Para obtener un archivo `manifest.yml` de muestra, consulte "Ejemplo de archivo manifest.yml" en la página 196.

Resultados
El recopilador de datos se ha configurado y está conectado al Servidor de Cloud APM.

Qué hacer a continuación

Puede verificar que los datos de la aplicación IBM Cloud se visualizan en la Consola de Cloud APM. Para obtener instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte Inicio de la consola de Cloud APM. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte Gestión de aplicaciones.

Recuerde: Para añadir su aplicación a la Consola de Cloud APM, elija **Node.js Runtime** en el editor de aplicaciones.

Personalización del recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud
Puede añadir variables de entorno en la interfaz de usuario de IBM Cloud para personalizar la supervisión de la aplicación IBM Cloud.

Variables de entorno definidas por el usuario para el recopilador de datos de Node.js

Puede utilizar la información de la tabla siguiente para personalizar la supervisión de Node.js en IBM Cloud.

Tabla 188. Variables de entorno definidas por el usuario soportadas para la supervisión de Node.js en IBM Cloud

Nombre de variable	Importancia	Valor	Descripción
KNJ_SAMPLING	Opcional	Recuento de solicitudes de muestreo	El número de solicitudes en función del cual se toma una muestra. El valor predeterminado es 10, lo que significa que se supervisa una de cada 10 solicitudes. Si no establece esta variable, se utiliza el valor predeterminado 10.
KNJ_MIN_CLOCK_TRACE	Opcional	Umbral de tiempo de respuesta para la recopilación de rastreo de método, en milisegundos	Si el tiempo de respuesta de una instancia de solicitud supera el valor de esta variable, el recopilador de datos recopila su rastreo de método. El valor predeterminado es 0. Si no establece esta variable, se utilizará el valor predeterminado 0.
KNJ_MIN_CLOCK_STACK	Opcional	Umbral de tiempo de respuesta para recopilar el rastreo de pila, en milisegundos	Si el tiempo de respuesta de una instancia de solicitud excede el valor de esta variable, el recopilador de datos recopila su seguimiento de la pila. El valor predeterminado es 0. Si no establece esta variable, se utilizará el valor predeterminado 0.

Tabla 188. Variables de entorno definidas por el usuario soportadas para la supervisión de Node.js en IBM Cloud (continuación)

Nombre de variable	Importancia	Valor	Descripción
KNJ_ENABLE_METHODTRACE	Opcional	• `True` • `False`	Habilita o inhabilita el rastreo de método. • Si establece esta variable en true, el rastreo de método para solicitudes se inhabilita. • Si establece este valor en false, el rastreo de método para las peticiones se habilita. Éste es el valor predeterminado. Si no establece esta variable, se utiliza el valor predeterminado `False` y rastreo de método para las solicitudes se habilita.
KNJ_ENABLE_DEEPDIVE	Opcional	• `True` • `False`	Si establece esta variable en true, los datos de diagnósticos se envían al servidor. De forma predeterminada, este valor se establece en false, lo que significa que los datos de diagnósticos no se envían al servidor.
KNJ_ENABLE_TT	Opcional	• `verdadero` • `falso`	Habilita o inhabilita el rastreo de transacciones de AAR. • Si establece esta variable en true, el rastreo de AAR está habilitado. • Si establece esta variable en false, el rastreo de transacciones de AAR está inhabilitado. De forma predeterminada, este valor no está establecido, lo que significa que el rastreo de transacciones está inhabilitado.

Tabla 188. Variables de entorno definidas por el usuario soportadas para la supervisión de Node.js en IBM Cloud (continuación)

Nombre de variable	Importancia	Valor	Descripción
KNJ_AAR_BATCH_FREQ	Opcional	Intervalo al que se envían los datos de AAR, en segundos	Especifica el intervalo de creación y envío de lotes de datos de AAR al servidor, en segundos. El valor predeterminado es 60, lo que significa que cada minuto se crean y se envían lotes de datos de AAR al servidor. **Nota:** Esta variable funciona con KNJ_AAR_BATCH_COUNT para determinar cuándo se crean y se envían lotes de datos de AAR al servidor. Cuando se cumple la condición establecida por una de las dos variables, se crean y se envían los lotes de datos de AAR. Cuando las solicitudes que los datos de AAR contienen alcanzan el número máximo, por ejemplo 100, en un intervalo inferior al establecido, se siguen creando y enviando lotes de datos inmediatamente.
KNJ_AAR_BATCH_COUNT	Opcional	Número máximo de solicitudes que un lote de datos de AAR contiene	Especifica el número máximo de solicitudes que un lote de datos de AAR puede contener antes de que se envíe al servidor. El valor predeterminado es 100, lo que significa que cuando el número de solicitudes que un lote de datos de AAR contiene alcanza 100, este lote de datos de AAR se envía al servidor.

Tabla 188. Variables de entorno definidas por el usuario soportadas para la supervisión de Node.js en IBM Cloud (continuación)

Nombre de variable	Importancia	Valor	Descripción
KNJ_LOG_LEVEL	Opcional	Nivel de información que se imprime en el registro	Controla el nivel de información que se imprime en el registro. Se proporcionan los niveles siguientes: **off** Los registros no se imprimen. **error** Solo se registra información si se da una condición de error. **info** Se registra información cuando el recopilador de datos del agente de Node.js se ejecuta normalmente. También se registran los datos de supervisión en bruto enviados al agente. **debug** Se anota información de depuración, información y error útil en el registro, por ejemplo, datos recopilados, datos que se envían al servidor y la respuesta del servidor. **all** Se anota toda la información en el registro. De forma predeterminada, el nivel de registro es `info`, lo que significa que la información de resumen sobre las acciones del recopilador de datos se imprime en el registro. Los registros se imprimen en la salida estándar.
SECURITY_OFF	Opcional	• `verdadero` • `falso`	Habilita o inhabilita la recopilación de información confidencial de usuario, como por ejemplo las cookies, el contexto de solicitud HTTP y el contexto de solicitud de base de datos. • Si establece esta variable en true, se recopila información confidencial. • Si establece esta variable en false, no se recopila información confidencial. Éste es el valor predeterminado. Si no especifica esta variable, se utiliza el valor predeterminado `false` y no se recopila información confidencial de usuario.

Desconfiguración del Recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud

Si no necesita supervisar el entorno de Node.js o si desea actualizar el Recopilador de datos de Node.js autónomo, primero debe desconfigurar los valores anteriores del Recopilador de datos de Node.js autónomo.

Procedimiento

1. Elimine la línea `require('ibmapm');` del archivo principal de la aplicación.

   Consejo: Si inicia la aplicación ejecutando el mandato **app.js**, `app.js` es el archivo principal de la aplicación.
2. Elimine las dependencias siguientes del archivo `package.json`.

   ```
   “ibmapm": "./ibmapm"
   ```

   Recuerde: No elimine las dependencias que la aplicación necesita.
3. Suprima la carpeta `ibmapm` del directorio de inicio de la aplicación.

Resultados

Ha desconfigurado satisfactoriamente el Recopilador de datos de Node.js autónomo.

Qué hacer a continuación

Tras desconfigurar el recopilador de datos, la Consola de Cloud APM continúa mostrando el recopilador de datos en cualquier aplicación a la que haya añadido el recopilador de datos. La Consola de Cloud APM mostrará que no hay datos disponibles para la aplicación y no indicará que el recopilador de datos está fuera de línea. Para obtener información sobre cómo eliminar el recopilador de datos de aplicaciones y de grupos de recursos, consulte “Eliminación de recopiladores de datos de Consola de Cloud APM” en la página 196.

Configuración del Recopilador de datos de Node.js autónomo para aplicaciones locales

Si ha instalado la aplicación Node.js en un entorno local, debe configurar el Recopilador de datos de Node.js para recopilar información sobre la aplicación Node.js.

Antes de empezar

1. Asegúrese de que la aplicación Node.js puede ejecutarse correctamente de forma local. El Recopilador de datos de Node.js autónomo puede supervisar Node.js V8.0.0 y fixpacks futuros, V10.0.0 y fixpacks futuros y V12.0.0 y fixpacks futuros.
2. Descargue el paquete de recopilador de datos del sitio web de IBM Marketplace. Para obtener instrucciones detalladas, consulte “Descarga de los agentes y recopiladores de datos” en la página 107.

Procedimiento

1. Extraiga los archivos del paquete del recopilador de datos. El paquete `nodejs_datacollector_8.1.4.0.6.tgz` está incluido en el directorio extraído.
2. Determine el directorio de inicio de la aplicación.
   - Para aplicaciones Node.js típicas, si utiliza el mandato **node app.js** para iniciar la aplicación Node.js y el archivo principal `app.js` se encuentra en el directorio `/root/nodejs_app`, el directorio de inicio de la aplicación es `/root/nodejs_app`.
   - Para miembros de colectivo en el entorno de IBM API Connect, ejecute el mandato **wlpn-server list** para visualizar la lista de todos los miembros de colectivo en la misma máquina. El directorio de inicio del miembro de colectivo está en el formato siguiente:

     ```
     directorio_usuario/nombre_miembro-colectivo/package
     ```

Por ejemplo, si obtiene `/root/wlpn/rock-8345a96-148538-1/package` como salida de mandato, `/root/wlpn` es el directorio de usuario y `rock-8345a96-148538-1` es el nombre de miembro de colectivo.

- Para aplicaciones de Developer Portal en el entorno de IBM API Connect, puede ejecutar el mandato **ps -ef | grep node** para encontrar el directorio de inicio. Si obtiene la salida de mandato siguiente, por ejemplo, el directorio de inicio es `/home/admin/bgsync` y el archivo principal de la aplicación es `rest_server.js`:

```
admin 19085 1 0 Jun25 ?  00:06:53 /usr/local/bin/node /home/admin/bgsync/
rest_server.js
```

3. En el directorio inicial de la aplicación, ejecute el mandato siguiente para extraer archivos del paquete recopilador de datos:

```
tar -zxf nodejs_datacollector_8.1.4.0.6.tgz
```

4. Extraiga el archivo `ibmapm.tgz` en la carpeta `nodejs_dc` ejecutando el mandato siguiente:

```
tar -zxf nodejs_dc/ibmapm.tgz
```

Obtendrá una carpeta `ibmapm`.

5. Ejecute el mandato siguiente para instalar el recopilador de datos en su aplicación:

```
npm install ./ibmapm
```

6. Añada la línea siguiente al principio del archivo principal de la aplicación Node.js:

```
require('ibmapm');
```

- Si inicia la aplicación ejecutando el mandato **app.js**, `app.js` es el archivo principal de la aplicación.
- Para miembros de colectivo en el entorno de IBM API Connect, el archivo principal está definido en el archivo `package.json`, en el directorio de inicio o en sus subcarpetas. De forma predeterminada, el archivo principal es *directorio_inicio*`/server/server.js`, donde *directorio_inicio* es el directorio de inicio del miembro de colectivo.
- Para aplicaciones de Developer Portal en el entorno de IBM API Connect, puede ejecutar el mandato **ps -ef | grep node** para buscar el archivo principal. Si obtiene la salida de mandato siguiente, por ejemplo, el archivo principal de la aplicación es `rest_server.js`.

```
admin 19085 1 0 Jun25 ?  00:06:53 /usr/local/bin/node /home/admin/bgsync/
rest_server.js
```

7. Reinicie la aplicación.

Consejo:

- Para reiniciar el miembro de colectivo, ejecute el mandato `wlpn-server stop` *nombre_miembro_colectivo*. El miembro de colectivo se reinicia automáticamente después de ejecutar este mandato. Si no se reinicia, ejecute el mandato `wlpn-server start` *nombre_miembro_colectivo* para reiniciarlo manualmente.
- Para reiniciar las aplicaciones de Developer Portal, ejecute primero el mandato `/etc/init.d/restservice stop` para detener la aplicación y a continuación ejecute el mandato `/etc/init.d/restservice start` para iniciarla.

Resultados

El recopilador de datos se ha configurado y está conectado al Servidor de Cloud APM.

Qué hacer a continuación

- Puede verificar que los datos de la aplicación se visualizan en la Consola de Cloud APM. Para obtener instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte Inicio de la consola de Cloud APM.

Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte Gestión de aplicaciones.

- Para información de topología para el entorno de API Connect, habilite el rastreo de transacciones. Para obtener más instrucciones, consulte la descripción de la variable *KNJ_ENABLE_TT* en "Personalización del Recopilador de datos de Node.js para aplicaciones locales" en la página 623.

Recuerde: Para añadir su aplicación a la Consola de Cloud APM, elija **Node.js Runtime** en el editor de aplicaciones.

Personalización del Recopilador de datos de Node.js para aplicaciones locales

Modificando los archivos del paquete de recopilador de datos, puede establecer las variables de entorno para personalizar la supervisión de la aplicación Node.js.

Puede establecer las variables personalizando las variables de entorno o editando el archivo `config.properties`. Encontrará el archivo `config.properties` en la carpeta `ibmapm/etc` en la que está instalado el recopilador de datos Node.js.

Tabla 189. Variables soportadas

Nombre de variable	Importancia	Valor	Descripción
KNJ_SAMPLING	Opcional	Recuento de solicitudes de muestreo	El número de solicitudes en función del cual se toma una muestra. El valor predeterminado es `10`, lo que significa que se supervisa una de cada 10 solicitudes. Si no establece esta variable, se utiliza el valor predeterminado `10`.
KNJ_MIN_CLOCK_TRACE	Opcional	Umbral de tiempo de respuesta para la recopilación de rastreo de método, en milisegundos	Si el tiempo de respuesta de una instancia de solicitud supera el valor de esta variable, el recopilador de datos recopila su rastreo de método. El valor predeterminado es `0`. Si no establece esta variable, se utilizará el valor predeterminado `0`.
KNJ_MIN_CLOCK_STACK	Opcional	Umbral de tiempo de respuesta para recopilar el rastreo de pila, en milisegundos	Si el tiempo de respuesta de una instancia de solicitud excede el valor de esta variable, el recopilador de datos recopila su seguimiento de la pila. El valor predeterminado es `0`. Si no establece esta variable, se utilizará el valor predeterminado `0`.

Tabla 189. Variables soportadas (continuación)

Nombre de variable	Importancia	Valor	Descripción
KNJ_ENABLE_METHODTRACE	Opcional	• `True` • `False`	Habilita o inhabilita el rastreo de método. • Si establece esta variable en true, el rastreo de método para solicitudes se inhabilita. • Si establece este valor en false, el rastreo de método para las peticiones se habilita. Éste es el valor predeterminado. Si no establece esta variable, se utiliza el valor predeterminado `False` y rastreo de método para las solicitudes se habilita.
KNJ_ENABLE_DEEPDIVE	Opcional	• `True` • `False`	Si establece esta variable en true, los datos de diagnósticos se envían al servidor. De forma predeterminada, este valor se establece en false, lo que significa que los datos de diagnósticos no se envían al servidor.
KNJ_ENABLE_TT	Opcional	• `verdadero` • `falso`	Habilita o inhabilita el rastreo de transacciones de AAR. • Si establece esta variable en true, el rastreo de AAR está habilitado. • Si establece esta variable en false, el rastreo de transacciones de AAR está inhabilitado. De forma predeterminada, este valor no está establecido, lo que significa que el rastreo de transacciones está inhabilitado.

Tabla 189. Variables soportadas (continuación)

Nombre de variable	Importancia	Valor	Descripción
KNJ_AAR_BATCH_FREQ	Opcional	Intervalo al que se envían los datos de AAR, en segundos	Especifica el intervalo de creación y envío de lotes de datos de AAR al servidor, en segundos. El valor predeterminado es 60, lo que significa que cada minuto se crean y se envían lotes de datos de AAR al servidor. **Nota:** Esta variable funciona con KNJ_AAR_BATCH_COUNT para determinar cuándo se crean y se envían lotes de datos de AAR al servidor. Cuando se cumple la condición establecida por una de las dos variables, se crean y se envían los lotes de datos de AAR. Cuando las solicitudes que los datos de AAR contienen alcanzan el número máximo, por ejemplo 100, en un intervalo inferior al establecido, se siguen creando y enviando lotes de datos inmediatamente.
KNJ_AAR_BATCH_COUNT	Opcional	Número máximo de solicitudes que un lote de datos de AAR contiene	Especifica el número máximo de solicitudes que un lote de datos de AAR puede contener antes de que se envíe al servidor. El valor predeterminado es 100, lo que significa que cuando el número de solicitudes que un lote de datos de AAR contiene alcanza 100, este lote de datos de AAR se envía al servidor.

Tabla 189. Variables soportadas (continuación)

Nombre de variable	Importancia	Valor	Descripción
KNJ_LOG_LEVEL	Opcional	Nivel de información que se imprime en el registro	Controla el nivel de información que se imprime en el registro. Se proporcionan los niveles siguientes: **off** Los registros no se imprimen. **error** Solo se registra información si se da una condición de error. **info** Se registra información cuando el recopilador de datos del agente de Node.js se ejecuta normalmente. También se registran los datos de supervisión en bruto enviados al agente. **debug** Se anota información de depuración, información y error útil en el registro, por ejemplo, datos recopilados, datos que se envían al servidor y la respuesta del servidor. **all** Se anota toda la información en el registro. De forma predeterminada, el nivel de registro es `info`, lo que significa que la información de resumen sobre las acciones del recopilador de datos se imprime en el registro. Los registros se imprimen en la salida estándar.
SECURITY_OFF	Opcional	• `verdadero` • `falso`	Habilita o inhabilita la recopilación de información confidencial de usuario, como por ejemplo las cookies, el contexto de solicitud HTTP y el contexto de solicitud de base de datos. • Si establece esta variable en true, se recopila información confidencial. • Si establece esta variable en false, no se recopila información confidencial. Éste es el valor predeterminado. Si no especifica esta variable, se utiliza el valor predeterminado `false` y no se recopila información confidencial de usuario.

Desconfiguración del Recopilador de datos de Node.js autónomo para aplicaciones locales

Si no necesita supervisar el entorno de Node.js o si desea actualizar el Recopilador de datos de Node.js autónomo, primero debe desconfigurar los valores anteriores del Recopilador de datos de Node.js autónomo.

Procedimiento

1. Elimine la línea `require('ibmapm');` del archivo principal de la aplicación.

   Consejo: Si inicia la aplicación ejecutando el mandato **app.js**, `app.js` es el archivo principal de la aplicación.
2. Elimine "`ibmapm": "./ibmapm"` de la sección de dependencias del archivo `package.json` de su aplicación Node.js.
3. Suprima la carpeta `node_modules` del directorio de inicio de la aplicación.
4. Ejecute el mandato `npm install` para instalar las dependencias de la aplicación.

Resultados

Ha desconfigurado satisfactoriamente el Recopilador de datos de Node.js autónomo.

Qué hacer a continuación

Tras desconfigurar el recopilador de datos, la Consola de Cloud APM continúa mostrando el recopilador de datos en cualquier aplicación a la que haya añadido el recopilador de datos. La Consola de Cloud APM mostrará que no hay datos disponibles para la aplicación y no indicará que el recopilador de datos está fuera de línea. Para obtener información sobre cómo eliminar el recopilador de datos de aplicaciones y de grupos de recursos, consulte "Eliminación de recopiladores de datos de Consola de Cloud APM" en la página 196.

Configuración del Recopilador de datos de Node.js autónomo para aplicaciones Kubernetes

Si ha instalado la aplicación Node.js en Kubernetes, puede configurar el Recopilador de datos de Node.js para recopilar información sobre la aplicación Node.js.

Antes de empezar

1. Asegúrese de que la aplicación Node.js se puede ejecutar satisfactoriamente. El Recopilador de datos de Node.js autónomo puede supervisar Node.js V8.0.0 y fixpacks futuros, V10.0.0 y fixpacks futuros y V12.0.0 y fixpacks futuros.
2. Descargue el paquete de recopilador de datos del sitio web de IBM Marketplace. Para obtener instrucciones detalladas, consulte "Descarga de los agentes y recopiladores de datos" en la página 107.

Procedimiento

1. Extraiga los archivos del paquete del recopilador de datos. El paquete `nodejs_datacollector_8.1.4.0.6.tgz` está incluido en el directorio extraído.
2. Extraiga el archivo `nodejs_datacollector_8.1.4.0.6.tgz`, por ejemplo, ejecutando el mandato siguiente:

   ```
   tar -zxf nodejs_datacollector_8.1.4.0.6.tgz
   ```
3. Extraiga el archivo `ibmapm.tgz` en la carpeta `nodejs_dc` ejecutando el mandato siguiente:

   ```
   tar -zxf nodejs_dc/ibmapm.tgz
   ```

   Obtendrá una carpeta `ibmapm`.
4. En el archivo `package.json` de la aplicación Node.js, añada la línea siguiente a la sección de dependencias:

```
"ibmapm": "./ibmapm"
```

Recuerde: no olvide especificar la coma al final de cada línea del archivo excepto la última, y mantener el formato correcto del archivo `package.json`.

5. Añada la línea siguiente al principio del archivo principal de la aplicación Node.js:

```
require('./ibmapm');
```

Si inicia la aplicación ejecutando el mandato **`app.js`**, `app.js` es el archivo principal de la aplicación.

6. Vuelva a crear la imagen de Docker.

Nota: Si ejecuta la aplicación Node.js en otros entornos de Docker, por ejemplo servicios de Docker Swarm o AWS Docker, debe utilizar Docker en los pasos.

Qué hacer a continuación
Si desea personalizar la supervisión, puede añadir variables de entorno en el archivo yaml de despliegue. Para obtener detalles, consulte "Personalización del recopilador de datos de Node.js autónomo para aplicaciones Kubernetes" en la página 628.

Personalización del recopilador de datos de Node.js autónomo para aplicaciones Kubernetes
Puede añadir variables de entorno al archivo yaml de despliegue para personalizar la supervisión de la aplicación Kubernetes.

Variables de entorno definidas por el usuario para el recopilador de datos de Node.js

Puede utilizar la información de la tabla siguiente para personalizar la supervisión de Node.js en Kubernetes.

Tabla 190. Variables de entorno definidas por el usuario soportadas para la supervisión de Node.js en Kubernetes

Nombre de variable	Importancia	Valor	Descripción
KNJ_SAMPLING	Opcional	Recuento de solicitudes de muestreo	El número de solicitudes en función del cual se toma una muestra. El valor predeterminado es `10`, lo que significa que se supervisa una de cada 10 solicitudes. Si no establece esta variable, se utiliza el valor predeterminado `10`.
KNJ_MIN_CLOCK_TRACE	Opcional	Umbral de tiempo de respuesta para la recopilación de rastreo de método, en milisegundos	Si el tiempo de respuesta de una instancia de solicitud supera el valor de esta variable, el recopilador de datos recopila su rastreo de método. El valor predeterminado es `0`. Si no establece esta variable, se utilizará el valor predeterminado `0`.

Tabla 190. Variables de entorno definidas por el usuario soportadas para la supervisión de Node.js en Kubernetes (continuación)

Nombre de variable	Importancia	Valor	Descripción
KNJ_MIN_CLOCK_STACK	Opcional	Umbral de tiempo de respuesta para recopilar el rastreo de pila, en milisegundos	Si el tiempo de respuesta de una instancia de solicitud excede el valor de esta variable, el recopilador de datos recopila su seguimiento de la pila. El valor predeterminado es `0`. Si no establece esta variable, se utilizará el valor predeterminado `0`.
KNJ_ENABLE_METHODTRACE	Opcional	• `True` • `False`	Habilita o inhabilita el rastreo de método. • Si establece esta variable en true, el rastreo de método para solicitudes se inhabilita. • Si establece este valor en false, el rastreo de método para las peticiones se habilita. Éste es el valor predeterminado. Si no establece esta variable, se utiliza el valor predeterminado `False` y rastreo de método para las solicitudes se habilita.
KNJ_ENABLE_DEEPDIVE	Opcional	• `True` • `False`	Si establece esta variable en true, los datos de diagnósticos se envían al servidor. De forma predeterminada, este valor se establece en false, lo que significa que los datos de diagnósticos no se envían al servidor.
KNJ_ENABLE_TT	Opcional	• `true` • `false`	Habilita o inhabilita el rastreo de transacciones de AAR. • Si establece esta variable en true, el rastreo de AAR está habilitado. • Si establece esta variable en false, el rastreo de transacciones de AAR está inhabilitado. De forma predeterminada, este valor no está establecido, lo que significa que el rastreo de transacciones está inhabilitado.

Tabla 190. Variables de entorno definidas por el usuario soportadas para la supervisión de Node.js en Kubernetes (continuación)

Nombre de variable	Importancia	Valor	Descripción
KNJ_AAR_BATCH_FREQ	Opcional	Intervalo al que se envían los datos de AAR, en segundos	Especifica el intervalo de creación y envío de lotes de datos de AAR al servidor, en segundos. El valor predeterminado es 60, lo que significa que cada minuto se crean y se envían lotes de datos de AAR al servidor. **Nota:** Esta variable funciona con KNJ_AAR_BATCH_COUNT para determinar cuándo se crean y se envían lotes de datos de AAR al servidor. Cuando se cumple la condición establecida por una de las dos variables, se crean y se envían los lotes de datos de AAR. Cuando las solicitudes que los datos de AAR contienen alcanzan el número máximo, por ejemplo 100, en un intervalo inferior al establecido, se siguen creando y enviando lotes de datos inmediatamente.
KNJ_AAR_BATCH_COUNT	Opcional	Número máximo de solicitudes que un lote de datos de AAR contiene	Especifica el número máximo de solicitudes que un lote de datos de AAR puede contener antes de que se envíe al servidor. El valor predeterminado es 100, lo que significa que cuando el número de solicitudes que un lote de datos de AAR contiene alcanza 100, este lote de datos de AAR se envía al servidor.

Tabla 190. Variables de entorno definidas por el usuario soportadas para la supervisión de Node.js en Kubernetes (continuación)

Nombre de variable	Importancia	Valor	Descripción
KNJ_LOG_LEVEL	Opcional	Nivel de información que se imprime en el registro	Controla el nivel de información que se imprime en el registro. Se proporcionan los niveles siguientes: **off** Los registros no se imprimen. **error** Solo se registra información si se da una condición de error. **info** Se registra información cuando el recopilador de datos del agente de Node.js se ejecuta normalmente. También se registran los datos de supervisión en bruto enviados al agente. **debug** Se anota información de depuración, información y error útil en el registro, por ejemplo, datos recopilados, datos que se envían al servidor y la respuesta del servidor. **all** Se anota toda la información en el registro. De forma predeterminada, el nivel de registro es `info`, lo que significa que la información de resumen sobre las acciones del recopilador de datos se imprime en el registro. Los registros se imprimen en la salida estándar.
SECURITY_OFF	Opcional	• `true` • `false`	Habilita o inhabilita la recopilación de información confidencial de usuario, como por ejemplo las cookies, el contexto de solicitud HTTP y el contexto de solicitud de base de datos. • Si establece esta variable en true, se recopila información confidencial. • Si establece esta variable en false, no se recopila información confidencial. Éste es el valor predeterminado. Si no especifica esta variable, se utiliza el valor predeterminado `false` y no se recopila información confidencial de usuario.

Ejemplo de archivo yaml

```
spec:
      containers:
      - name: testapp
        image: mycluster.icp:8500/default/testapp:v1
        imagePullPolicy: Always
        ports:
        - containerPort: 3000
          protocol: TCP
        env:        - name: KNJ_LOG_LEVEL
          value: "debug"
        - name: KNJ_ENABLE_TT
          value: "true"
        - name: KNJ_ENABLE_DEEPDIVE
          value: "true"
```

Desconfiguración del Recopilador de datos de Node.js autónomo para aplicaciones Kubernetes
Si no necesita supervisar el entorno de Node.js o si desea actualizar el Recopilador de datos de Node.js autónomo, primero debe desconfigurar los valores anteriores del Recopilador de datos de Node.js autónomo.

Procedimiento

1. Elimine la línea `require('ibmapm');` del archivo principal de la aplicación.

   Consejo: Si inicia la aplicación ejecutando el mandato **app.js**, `app.js` es el archivo principal de la aplicación.
2. Elimine las dependencias siguientes del archivo `package.json`.

   ```
   "ibmapm": "./ibmapm"
   ```

   Recuerde: No elimine las dependencias que la aplicación necesita.

Resultados
Ha desconfigurado satisfactoriamente el Recopilador de datos de Node.js autónomo.

Qué hacer a continuación
Tras desconfigurar el recopilador de datos, la Consola de Cloud APM continúa mostrando el recopilador de datos en cualquier aplicación a la que haya añadido el recopilador de datos. La Consola de Cloud APM mostrará que no hay datos disponibles para la aplicación y no indicará que el recopilador de datos está fuera de línea. Para obtener información sobre cómo eliminar el recopilador de datos de aplicaciones y de grupos de recursos, consulte “Eliminación de recopiladores de datos de Consola de Cloud APM” en la página 196.

Configuración de la supervisión de OpenStack

Debe configurar el Monitoring Agent for OpenStack para que el agente pueda supervisar automáticamente el entorno del Agente de OpenStack.

Procedimiento

1. Configurar el agente respondiendo a solicitudes. Para obtener instrucciones, consulte “Configuración del Agente de OpenStack” en la página 633.
2. Si desea recopilar información relacionada con el proceso, configure el recopilador de datos del Agente de OpenStack. Para obtener instrucciones, consulte “Habilitación de la recopilación de información relacionada con procesos y de conexiones SSH” en la página 635.
3. Especifique valores de configuración para que el agente funcione. Para obtener instrucciones, consulte “Adición de los valores de configuración” en la página 636.

Configuración del Agente de OpenStack

Para un entorno típico, si desea que el Agente de OpenStack supervise automáticamente el entorno OpenStack, debe configurar primero el agente.

Antes de empezar

Asegúrese de haber instalado todo el software necesario como se describe en Preinstalación en sistemas Linux.

Procedimiento

Tiene dos opciones para configurar el Agente de OpenStack en un sistema Linux:

- Para configurar el agente mediante la ejecución del script y las respuestas a las solicitudes, consulte "Configuración interactiva" en la página 633.
- Para configurar el agente mediante la edición del archivo de respuestas silenciosas y la ejecución del script sin interacción, consulte "Configuración silenciosa" en la página 634.

Configuración interactiva

Procedimiento

1. Para configurar el agente, ejecute el mandato siguiente:

   ```
   dir_instalación/bin/openstack-agent.sh config nombre_instancia
   ```

   donde *dir_instalación* es el directorio de instalación del Agente de OpenStack. El directorio de instalación predeterminado es `/opt/ibm/apm/agent`.
2. Cuando se le solicite `Especificar un nombre de instancia`, especifique un nombre de instancia.

   Importante: El Agente de OpenStack es un agente de varias instancias y necesita un nombre de instancia para cada instancia de agente. El nombre de instancia especificado se incluirá en el nombre del sistema gestionado, `nombre_instancia:nombre_host:sg`. La longitud del nombre de instancia que especifique está limitada a 28 caracteres menos la longitud del nombre de host. Por ejemplo, si especifica `OS1` como nombre de instancia, el nombre de sistema gestionado será `OS1:nombrehost:PN`.
3. Cuando se le solicite `Editar Monitoring Agent for OpenStack`, pulse `Intro` para continuar.
4. Cuando se le solicite `Editar información de autenticación de entorno de OpenStack`, proporcione la información siguiente:

   ```
   URL de autenticación de OpenStack (el valor predeterminado es: http://localhost:identity/v3):
   Nombre de usuario de OpenStack (el valor predeterminado es: admin):
   Especificar contraseña de OpenStack (el valor predeterminado es: ):
   Volver a especificar: contraseña de OpenStack (el valor predeterminado es: ):
   Nombre de arrendatario de OpenStack (el valor predeterminado es: admin):
   ```
5. Cuando se le solicite la `Ubicación de ejecutable de Python`, especifique la ubicación del ejecutable de Python, por ejemplo, `/usr/bin/python`.

   Encontrará la vía de acceso completa ejecutando el mandato siguiente en el entorno:

   ```
   which python
   ```
6. Cuando se le solicite `Número de puerto`, acepte el valor predeterminado o especifique un número de puerto.

   Este puerto se utiliza para supervisar la comunicación interna entre el recopilador de datos del Agente de OpenStack y el Agente de OpenStack, estando ambos instalados solo en un servidor local. El agente está a la escucha en este puerto de datos del recopilador de datos. El valor predeterminado 0 indica que se utiliza un puerto efímero cuando se inicia el agente. En un servidor con reglas de seguridad estrictas sobre los puertos, puede configurar un puerto específico para que lo utilice el

agente. Este puerto es solo para uso interno del agente y no está relacionado con el entorno de OpenStack.

7. Edite el archivo `/etc/hosts` en el sistema para añadir correlación de hosts para cada nodo supervisado.

Configuración silenciosa

Procedimiento

1. Abra el archivo `sg_silent_config.txt` en un editor de texto. El archivo está en el directorio *`dir_instalación`*`/samples`, donde *dir_instalación* es el directorio de instalación del Agente de OpenStack.
2. Edite el archivo de configuración de `sg_silent_config.txt` del Agente de OpenStack.
3. Especifique valores para los parámetros identificados en el archivo. El archivo de respuestas contiene comentarios que definen los parámetros disponibles y los valores a especificar.
4. Guarde el archivo y salga.
5. Edite el archivo `/etc/hosts` en el sistema para añadir correlación de hosts para cada nodo supervisado.
6. En el directorio *`dir_instalación`*`/samples` ejecute el mandato siguiente para configurar el agente:

   ```
   dir_instalación/bin/openstack-agent.sh config nombre_instancia vía_acceso_archivo_respuestas
   ```

   donde *dir_instalación* es el nombre de la instancia que debe configurarse, y *vía_acceso_archivo_respuestas* es la vía de acceso completa del archivo de respuestas silencioso. Especifique una vía de acceso absoluta a este archivo.

   Por ejemplo, si el archivo de respuestas está en el directorio predeterminado, ejecute el mandato siguiente.

   ```
   /opt/ibm/apm/agent/bin/openstack-agent.sh config nombre_instancia
   /opt/ibm/apm/agent/samples/sg_silent_config.txt
   ```

Resultados
El agente está configurado.

Qué hacer a continuación

- Después de terminar de configurar el agente, puede iniciar la instancia del agente ejecutando el mandato:

  ```
  dir_instalación/bin/openstack-agent.sh start nombre_instancia
  ```

  donde *nombre_instancia* es el nombre de la instancia de agente que debe configurarse.
- Para conectar Agente de OpenStack con un entorno OpenStack habilitado para SSL, especifique el directorio del certificado SSL de servidor OpenStack estableciendo la variable siguiente:

  ```
  OS_cert_path=directorio del archivo certificate.crt
  ```

  La variable `OS_cert_path` está en la sección `OS_authentication_info` en el archivo `ksg_dc_`*`nombre_instancia`*`.cfg`.
- Si desea recopilar información relacionada con el proceso, configure el recopilador de datos del Agente de OpenStack siguiendo los pasos de "Habilitación de la recopilación de información relacionada con procesos y de conexiones SSH" en la página 635.
- Si desea cambiar el nivel de rastreo del agente a efectos de resolución de problemas, edite el valor de la variable **KBB_RAS1** en el archivo *`dir_instalación`*`/config/sg.environment` según las instrucciones del archivo.

Habilitación de la recopilación de información relacionada con procesos y de conexiones SSH

Si desea recopilar información relacionada con procesos, configure el recopilador de datos de agente para Agente de OpenStack y configure conexiones SSH con el servidor de componentes de OpenStack de destino.

Acerca de esta tarea

Debe configurar una conexión SSH para recopilar información de proceso antes de iniciar el Agente de OpenStack. Para configurar la conexión, utilice la herramienta de asistencia **ksg_setup_key.sh** o **ksg_ssh_setup.py** proporcionada por el producto y descrita en el procedimiento siguiente.

Si está familiarizado con la configuración de conexiones SSH, también puede utilizar los mandatos de Linux **ssh-keygen** y **ssh-copy-id** para configurar la conexión.

Procedimiento

1. Vaya al directorio *dir_instalación*/config, donde *dir_instalación* es el directorio de instalación del agente.
2. Edite el archivo ksg_dc_*nombre_instancia*.cfg, donde *nombre_instancia* es el nombre especificado para esta instancia de agente.

   El archivo se crea una vez iniciada la instancia de agente. Si el archivo no existe, copie *dir_instalación*/lx8266/sg/bin/ksg_dc.cfg en el directorio *dir_instalación*/config y cambie el nombre de archivo a ksg_dc_*nombre_instancia*.cfg.

   Por ejemplo, si el nombre de instancia es OS1, cambie el nombre a ksg_dc_OS1.cfg.
3. En el archivo ksg_dc_*nombre_instancia*.cfg, establezca el valor del parámetro **collect_process_information** en YES.
4. En la sección **OS_process_collection**, especifique el valor del parámetro **ssh_user_host** con los usuarios y nombres de host o direcciones IP de los servidores de componente de OpenStack según el formato del ejemplo siguiente:

   ```
   ssh_user_host=root@9.112.250.248,user1@hostname
   ```
5. Guarde los valores.
6. Para que los valores entren en vigor, reinicie la instancia de agente ejecutando los mandatos siguientes:

   ```
   dir_instalación/bin/openstack-agent.sh stop nombre_instancia
   dir_instalación/bin/openstack-agent.sh start nombre_instancia
   ```
7. Configure las conexiones SSH con el servidor de componentes de destino de una de las maneras siguientes:
   - Configure las conexiones una por una mediante el script ksg_setup_key.sh: vaya al directorio *dir_instalación*/lx8266/sg/bin y ejecute el script ksg_setup_key.sh con el nombre de host o la IP y el usuario para crear las conexiones SSH con los servidores de componente especificados en el paso 4. Si sigue el ejemplo que se proporciona en el paso 4, debe ejecutar el script dos veces para configurar la conexión una a una:

     ```
     ./ksg_setup_key.sh 9.112.250.248 root
     ./ksg_setup_key.sh hostname user1
     ```

     Nota: Debe proporcionar las contraseñas cuando ejecuta los scripts por primera vez. No es necesario volver a proporcionar las contraseñas.
   - Configure las conexiones una a una o en un trabajo de proceso por lotes mediante la herramienta ksg_ssh_setup.py proporcionada por el Agente de OpenStack en *dir_instalación*/lx8266/sg/bin. Debe instalar la biblioteca pexpect de Python para poder utilizar esta herramienta.
     – Para configurar las conexiones SSH una a una, ejecute el mandato:

```
python ksg_ssh_setup.py -single
```

Este mandato le ayuda a configurar la conexión SSH con el servidor de destino remoto. Debe proporcionar la siguiente información:

```
Especifique el nombre de host o la dirección IP de la maquina de destino remota:
(teclee 'END' para finalizar la entrada.)
Especifique la cuenta de acceso a la máquina remota (p. ej. root):
Especifique la contraseña del usuario anterior:
```

– Para configurar conexiones SSH en un trabajo por lotes, ejecute el mandato:

```
python ksg_ssh_setup.py -ssh archivo_SSH
```

donde *archivo_SSH* es el archivo que contiene la información de servidor de destino, usuario y contraseña. Debe crear el archivo según el archivo `ksg_dc_ssh_list.txt` que hay en el mismo directorio que la herramienta Python y especificar la información de host y usuario según el formato de los ejemplos:

```
hostname root passw0rd
9.112.250.248 user1 passw0rd
```

Nota: solo debe volver a configurar las conexiones cuando cambian el nombre de usuario o la contraseña del servidor de destino. No es necesario volver a configurar las conexiones después de reiniciar el agente o cambiar la configuración del agente.

Resultados

El recopilador de datos está configurado y las conexiones SSH se han configurado adecuadamente. Ahora puede iniciar la sesión en la consola de Cloud APM y utilizar el editor de aplicaciones para añadir la instancia de Agente de OpenStack al Panel de instrumentos del rendimiento de aplicaciones. Al añadir la instancia de agente, elija **Entorno de OpenStack** en la lista de componentes al añadir la instancia del agente.

Qué hacer a continuación

- Cuando pulsa **Resumen de puntos finales de la API por tipo de servicio** > **Detalles de punto final de la API**, verá un mensaje `No hay datos disponibles` en los widgets de grupo **Historial de Tiempos de errores de detección de la API** y **Historial de Porcentaje de errores de detección de la API**. Pulse un punto final de la API que se muestre en **Detalles de punto final de la API** y podrá ver datos de supervisión en los dos widgets de grupo.
- Cuando pulsa **Resumen de procesos por componente** > **Detalles de proceso** o **Estado de conexión del servidor SSH** > **Detalles de proceso**, verá un mensaje `No hay datos disponibles` en los widgets de grupo **Historial de uso de CPU de proceso** e **Historial de uso de memoria de proceso**. Pulse sobre un proceso que se muestre en **Detalles de proceso** y podrá ver datos de supervisión en los dos widgets de grupo.

Adición de los valores de configuración

Para la configuración local y remota, debe proporcionar los valores de configuración para que el agente funcione.

Cuando utiliza la modalidad interactiva para configurar el agente, se visualiza un panel para que pueda especificar cada valor. Cuando existe un valor predeterminado, este valor aparece en el campo. Si un campo representa una contraseña, se visualizan dos campos de entrada. Debe especificar el mismo valor en cada campo. Los valores que teclea no se muestran a fin de mantener la seguridad de dichos valores.

Cuando utiliza la modalidad silenciosa para configurar el agente, puede editar el *archivo_respuestas* en el directorio *dir_instalación*`/samples` para añadir los valores de configuración. Después de

guardar los cambios, siga las instrucciones del paso “6” en la página 634 y ejecute el mandato siguiente para que los cambios entren en vigor:

```
dir_instalación/bin/openstack-agent.sh start nombre_instancia
```

donde *nombre_instancia* es el nombre de la instancia de agente que debe configurarse.

Una vez realizada la configuración, encontrará los valores configurados en el archivo `.cfg` de la instancia de agente, por ejemplo *nombre_host*`_sg_`*nombre_instancia*`.cfg`.

La configuración para este agente está organizada en las siguientes grupos:

Información de autenticación de entorno de OpenStack (OPENSTACK_CONNECTION)
La información de autenticación de entorno de OpenStack

Los elementos de configuración definidos en este grupo están siempre presentes en la configuración del agente.

Este grupo define información que se aplica a todo el agente.

URL de autenticación de OpenStack (KSG_OPENSTACK_AUTH_URL)
El URL de autenticación de entorno de OpenStack

El tipo es serie.

Este valor es obligatorio.

Valor predeterminado: `http://localhost:identity/v3`

Contraseña de OpenStack (KSG_OPENSTACK_PASSWORD)
La contraseña del usuario administrador

El tipo es contraseña.

Este valor es obligatorio.

Valor predeterminado: ninguno

Nombre de arrendatario de OpenStack (KSG_OPENSTACK_TENANT_NAME)
El nombre de arrendatario de OpenStack, también conocido como nombre de proyecto

El tipo es serie.

Este valor es obligatorio.

Valor predeterminado: admin

Nombre de usuario de OpenStack (KSG_OPENSTACK_USERNAME)
Usuario administrador para iniciar sesión en el entorno de OpenStack

El tipo es serie.

Este valor es obligatorio.

Valor predeterminado: admin

Python (KSG_PYTHON)
Ubicación del ejecutable de Python

Los elementos de configuración definidos en este grupo están siempre presentes en la configuración del agente.

Este grupo define información que se aplica a todo el agente.

Ubicación del ejecutable de Python (KSG_PYTHON_LOCATION)
El ejecutable de python que se utilizar´para ejecutar el recopilador de datos del agente de OpenStack. Encontrará la ruta completa si ejecuta el siguiente mandato en su terminal: "which python".

El tipo es serie.

Este valor es obligatorio.

Valor predeterminado: ninguno

Socket (KSG_SOCKET)
Origen de datos de socket

Los elementos de configuración definidos en este grupo están siempre presentes en la configuración del agente.

Este grupo define información que se aplica a todo el agente.

Número de puerto (CP_PORT)
El puerto que utilizará el agente para escuchar los datos desde los clientes de socket. Un valor de 0 indica que se utilizará un puerto efímero. Este puerto NO se corresponde con ninguno de los puertos utilizados por la aplicación. Este puerto es para uso interno del agente.

El tipo es numérico.

Este valor es opcional.

Valor predeterminado: 0

Configuración de la supervisión de base de datos de Oracle

El Monitoring Agent for Oracle Database proporciona prestaciones de supervisión para la disponibilidad, el rendimiento y el uso de recursos del entorno de base de datos Oracle. Puede configurar más de una instancia de Agente de Oracle Database para supervisar diferentes bases de datos de Oracle. Este agente también proporciona la capacidad de supervisión remota.

Antes de empezar

- Antes de configurar el Agente de Oracle Database, debe otorgar privilegios a la cuenta de usuario de Oracle utilizada por el Agente de Oracle Database. Para obtener más información sobre los privilegios, consulte la sección Otorgar privilegios al usuario de agente de base de datos Oracle.
- Si está supervisando una base de datos Oracle de forma remota, el agente debe estar instalado en un sistema que tenga instalado el software de base de datos Oracle o el cliente de Oracle Instant.

Acerca de esta tarea

Las instrucciones siguientes son para el release más reciente del agente, a excepción de lo indicado. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Versión de agente.

Para la supervisión del rendimiento global de la base de datos Oracle, el Agente de Oracle Database proporciona supervisión de la disponibilidad, el rendimiento, la utilización de recursos y las actividades de la base de datos Oracle, por ejemplo:

- Disponibilidad de instancias en la base de datos Oracle supervisada.
- Información de recursos como la memoria, la memorias caché, segmentos, limitación de recursos, espacio de tabla, deshacer (retrotracción), métricas del sistema y estadísticas del sistema.
- Información de actividades, como por ejemplo estadísticas de sistema operativo, sesiones, contención y registro de alertas.

El Agente de Oracle Database es un agente de varias instancias. Deberá crear la primera instancia e iniciar el agente manualmente. Además, cada instancia de agente puede supervisar varias bases de datos.

El Nombre de sistema gestionado del Agente de Oracle Database incluye un nombre de conexión de base de datos especificado por el usuario, un nombre de instancia especificado por el usuario y el nombre de host del sistema en el que está instalado el agente. Por ejemplo, `pc:nombre_conexión-nombre_instancia-nombre_host:SUB`, donde *pc* es el código del producto de dos caracteres y *SUB* es el tipo de base de datos (los valores posibles son RDB, ASM o DG). El Nombre de sistema gestionado está limitado a 32 caracteres. El nombre de instancia que especifique está limitado a 23 caracteres

menos la longitud del nombre de host y la conexión de base de datos. Por ejemplo, si especifica **dbconn** como nombre de conexión de base de datos, **Oracle02** como su nombre de instancia de agente y su nombre de host es *Prod204a*, el nombre de sistema gestionado es `RZ:dbconn-oracle02-Prod204a:RDB`. Este ejemplo utiliza 22 de los 23 caracteres disponibles para el nombre de conexión de base de datos, el nombre de instancia de agente y el nombre de host.

- Si especifica un nombre de instancia largo, el Nombre de sistema gestionado queda truncado y el código de agente no se visualiza correctamente.
- La longitud de las variables *nombre_conexión*, *nombre_instancia* y *nombre_host* se truncan cuando superan los 23 caracteres.
- Para evitar que un nombre de subnodo se trunque, modifique el convenio de denominación de subnodo configurando las siguientes variables de entorno: **KRZ_SUBNODE_INCLUDING_AGENTNAME**, **KRZ_SUBNODE_INCLUDING_HOSTNAME** y **KRZ_MAX_SUBNODE_ID_LENGTH**.
- Si establece **KRZ_SUBNODE_INCLUDING_AGENTNAME** en `NO`, la parte del ID de subnodo del nombre de subnodo no incluirá el nombre de instancia de agente. Por ejemplo,
  - Nombre de subnodo predeterminado: *DBConnection-Instancia-Nombre_host*
  - Nombre de subnodo con la variable de entorno establecida en `NO`: *DBConnection-Nombre_host*
- Si establece **KRZ_SUBNODE_INCLUDING_HOSTNAME** en `NO`, la parte del ID de subnodo del nombre de subnodo no incluye el nombre de host. Por ejemplo,
  - Nombre de subnodo predeterminado: *DBConnection-Instancia-Nombre_host*
  - Nombre de subnodo con la variable de entorno establecida en `NO`: *DBConnection-Instancia*

Procedimiento

1. Para configurar el agente en sistemas Windows, puede utilizar la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
   - "Configuración del agente en sistemas Windows" en la página 640.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 648.
2. Para configurar el agente en sistemas Linux y UNIX, puede ejecutar el script y responder a solicitudes o utilizar el archivo de respuestas silencioso.
   - "Configuración del agente respondiendo a solicitudes" en la página 644.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 648.

Qué hacer a continuación

Sólo para una configuración avanzada, el administrador de bases de datos Oracle debe permitir que el usuario de Oracle ejecute el script `krzgrant.sql` para acceder a la base de datos; consulte la sección Ejecución del script krzgrant.sql.

En la Consola de Cloud APM, vaya al Panel de instrumentos del rendimiento de aplicaciones para ver los datos que se han recopilado. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si no puede ver los datos en los paneles de instrumentos del agente, consulte primero los registros de conexión del servidor y, a continuación, los registros del proveedor de datos. Las vías de acceso predeterminadas a estos registros son los siguientes:

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Si desea recibir ayuda con la resolución de problemas, consulte el Foro de Cloud Application Performance Management.

Configuración del agente en sistemas Windows

Puede configurar el agente en sistemas operativos Windows mediante la ventana **IBM Performance Management**. Después de actualizar los valores de configuración, inicie el agente para guardar los valores actualizados.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la plantilla **Monitoring Agent for Oracle Database** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar una instancia de agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar la instancia de agente de nuevo, púlsela con el botón derecho del ratón y luego pulse **Reconfigurar**.
3. En la ventana Monitoring Agent for Oracle Database, realice los pasos siguientes:
   a) Escriba un nombre exclusivo para la instancia del Monitoring Agent for Oracle Database y pulse **Aceptar**.
4. En el panel Configuración de base de datos predeterminada de la ventana **Configurar ITCAM Extended Agent for Oracle Database**, siga estos pasos:
   a) Especifique el **`Nombre de usuario predeterminado`**. Este es el ID de usuario de base de datos predeterminado para las conexiones de base de datos.

      Este ID de usuario es el ID que el agente utiliza para acceder a la instancia de base de datos supervisada. Este ID de usuario debe tener privilegios de selección en las vistas y tablas de rendimiento dinámicas que son necesarias para el agente.
   b) Especifique la **`Contraseña predeterminada`**. Esta es la contraseña que está asociada con el ID de usuario de base de datos predeterminado especificado.
   c) Si la versión del agente de Oracle es 8.0, realice este paso.
      1) Especifique el **`Archivo Jar JDBC de Oracle`**. Esta es la vía de acceso completa al archivo jar del controlador JDBC de Oracle utilizado para comunicarse con la base de datos Oracle. El controlador JDBC (Java Database Connectivity) de Oracle controlador que da soporte a las versiones de base de datos de Oracle supervisadas por el agente de Oracle debe estar disponible en el sistema del agente.
   d) Si la versión del agente de Oracle es 6.3.1.10, siga estos pasos.
      1) Si el Agente de Oracle Database está instalado en el servidor de bases de datos Oracle que se supervisa, seleccione **Utilizar bibliotecas del directorio inicial de Oracle** y especifique el **`Directorio inicial de Oracle`**. Opcionalmente, para la supervisión local, el valor de `Directorio inicial de Oracle` puede dejarse en blanco para que se utilice la variable de entorno del sistema *ORACLE_HOME*.
      2) Si el Agente de Oracle Database es remoto con respecto al servidor de bases de datos Oracle que se supervisa, seleccione **Utilizar bibliotecas del cliente de Oracle instant** y especifique el **`Directorio de instalación del cliente de Oracle Instant`**.
   e) Si necesita opciones de configuración avanzadas, seleccione **Mostrar opciones avanzadas**; de lo contrario, continúe en el paso 5.
   f) `Directorios de archivos de configuración de red` puede dejarse en blanco para que se utilice el directorio predeterminado. Si la versión del agente de Oracle es 6.3.1.10, puede especificar varios directorios de archivos de configuración de red utilizando signos de punto y coma (;) para separar los directorios. En la versión del agente de Oracle 8.0, sólo se admite un directorio.

      Este valor contiene el archivo o archivos de configuración de red de la base de datos Oracle. El directorio lo define la variable de entorno *TNS_ADMIN* para cada instancia de base de datos Oracle. El directorio predeterminado es `%ORACLE_HOME%\NETWORK\ADMIN`. Si no se configura este valor, se utiliza el directorio predeterminado. Para inhabilitar el uso del directorio predeterminado, establezca la siguiente variable de entorno del agente en false: `KRZ_LOAD_ORACLE_NET=false`.

g) Deje el `Nombre de archivo de definición de SQL personalizado` en blanco. No se utiliza.

h) Elija si el escucha dinámico predeterminado está configurado en esta estación de trabajo.

El escucha dinámico predeterminado es `(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)`. Si el escucha dinámico predeterminado está configurado en esta estación de trabajo, establezca este valor en Yes.

i) Pulse **Siguiente**.

5. En el panel **Configuración de instancia** de la ventana **Configurar ITCAM Extended Agent for Oracle Database**, siga estos pasos:

aquí es donde se definen las instancias de conexión a base de datos reales. Debe añadir como mínimo una. También aquí se editan y suprimen las instancias de conexión de base de datos. Si existen varias configuraciones de instancia de conexión a base de datos, utilice la opción **Conexiones de base de datos** para elegir la instancia que debe editarse o suprimirse.

a) Pulse **Nuevo** en la sección **`Conexiones de base de datos`**.

b) Especifique un **`Nombre de conexión a base de datos`** como un alias para la conexión con la base de datos.

Este alias puede ser cualquier cosa que elija para representar la conexión a base de datos, con las limitaciones siguientes. Sólo se pueden utilizar letras, números arábigos, el carácter de subrayado y el símbolo "menos" en el nombre de la conexión. La longitud máxima de un nombre de conexión son 25 caracteres.

c) Elija un **`Tipo de conexión`**

1) (Opcional) Básica

El tipo de conexión predeterminado y más habitual es **Básica**. Si no está seguro del tipo de conexión necesario, es aconsejable elegir este tipo de conexión.

a) Seleccione el tipo de conexión **Básica** cuando la base de datos supervisada de destino sea una sola instancia, como por ejemplo una instancia de sistema de archivos estándar o una sola instancia de ASM.

b) Especifique el `Nombre de host` como nombre de host o dirección IP de la base de datos.

c) Especifique el `Puerto` utilizado por la base de datos.

d) Seleccione **Nombre de servicio** o **SID**.

i. Si ha seleccionado **Nombre de servicio**, especifique el nombre del servicio que es una representación lógica de una base de datos, una serie de caracteres que es el nombre del servicio de base de datos global.

Un nombre de servicio es una representación lógica de una base de datos, que es la forma en que la base de datos se presenta a los clientes. Una base de datos puede presentarse en forma de varios servicios, y un servicio puede implementarse en forma de varias instancias de base de datos. El nombre de servicio es una serie que es el nombre de base de datos global, es decir, un nombre formado por el nombre de base de datos y el nombre de dominio, especificado durante la instalación o la creación de la base de datos. Si no está seguro de cuál es el nombre de base de datos global, puede obtenerlo a partir del valor del parámetro SERVICE_NAMES del archivo de parámetros de inicialización.

ii. Si se ha seleccionado **SID**, especifique el identificador de sistema Oracle que identifica una instancia específica de una base de datos en ejecución.

Este es el identificador de sistema Oracle que identifica una instancia específica de una base de datos.

Continúe en el paso 5d.

2) (Opcional) TNS

a) Seleccione el tipo de conexión **TNS** si se ha establecido la variable de entorno de sistema *ORACLE_HOME HOME* y el alias de TNS para la base de datos supervisada de destino está definido en el archivo `$ORACLE_HOME/network/admin/tnsnames.ora`.

b) Especifique el nombre de **`Alias de TNS`**.

Continúe en el paso 5d.

3) (Opcional) Avanzada

a) Seleccione el tipo de conexión **Avanzada** cuando haya más de una instancia de Oracle en varios nodos físicos para la base de datos de destino supervisada. Por ejemplo, una base de datos ASM con RAC (Real Applications Cluster).

b) Especifique la **`Serie de conexión de Oracle`**.

Este atributo soporta todos los métodos de denominación de Oracle Net de la siguiente manera:

- Serie de URL de conexión SQL con el formato: `//host:puerto/nombre de servicio`. Por ejemplo, `//dlsun242:1521/bjava21`.
- Par palabra clave-valor de Oracle Net. Por ejemplo,

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=bjava21)))
```

- Entradas **TNSNAMES**, como por ejemplo **inst1,** con la variable de entorno *TNS_ADMIN* o *ORACLE_HOME* establecida y los archivos de configuración configurados.

Continúe en el paso 5d.

d) Seleccione **Utilizar un nombre de usuario y contraseña diferentes** para que esta conexión utilice credenciales diferentes a las predeterminadas que ha establecido en el paso 4a y el paso 4b. De lo contrario, continúe en el paso 5g.

e) Especifique el **`Nombre de usuario de base de datos`** para esta conexión.

Este ID de usuario es el ID que el agente utiliza para acceder a la instancia de base de datos supervisada. Este ID de usuario debe tener privilegios de selección en las vistas y tablas de rendimiento dinámicas que son necesarias para el agente.

f) Especifique la **`Contraseña de base de datos`**. Es la contraseña que está asociada con el ID de usuario de base de datos especificado.

g) Seleccione un **Rol** que coincida con los permisos otorgados a las credenciales de la conexión a base de datos.

El rol es el conjunto de privilegios que deben asociarse con la conexión. Para un usuario con el privilegio del sistema SYSDBA, especifique un rol que incluya ese privilegio. Para instancias de ASM, utilice el rol **SYSDBA** o **SYSASM**.

h) Seleccione **Mostrar opciones de supervisión de registro remoto** si supervisa registros de alertas de Oracle remotos desde esta instancia de agente; de lo contrario, continúe en el paso 5k.

i) Especifique una vía de acceso o utilice **Examinar** para seleccionar las **`Vías de acceso del archivo de registro de alertas Oracle`**.

Las vías de acceso de archivo absolutas de archivos de registro de alertas correlacionados para instancias de base de datos remotas en esta conexión de base de datos. El agente supervisa el registro de alertas leyendo estos archivos. Normalmente, se encuentran en `$ORACLE_BASE/diag/rdbms/`*`NOMBRE_BD`*`/`*`SID`*`/trace/alert_`*`SID`*`.log`. Por ejemplo si *DB_NAME* y *SID* son db11g, y *ORACLE_BASE* es `/home/dbowner/app/oracle`, el registro de alertas se encontrará en `/home/dbowner/app/oracle/diag/rdbms/db11g/db11g/trace/alert_db11g.log`.

Windows Si el Agente de Oracle Database se ejecuta y lee los archivos de registro de alertas a través de la red, la vía de acceso del archivo remoto debe cumplir los convenios de denominación universal de sistemas Windows. Por ejemplo, `\\tivx015\path\alert_orcl.log`.

Windows

Importante: Especifique la vía de acceso y el nombre del archivo de registro de alertas juntos. Una vía de acceso del registro de alertas no soporta el controlador de red correlacionado.

Linux AIX Si el Agente de Oracle Database se encuentra en un servidor remoto, se necesita un sistema de archivos montado localmente para supervisar sus registros de alertas remotas.

Windows Los diversos archivos se separan con un punto y coma (;).

Linux AIX Los diversos archivos se separan con dos puntos (:).

Cada archivo se compara con una instancia de base de datos mediante el patrón de nombre de archivo `alert_`*`instancia`*`.log` o, si no coincide, se ignora.

Los registros de alertas de la instancia de base de datos local se descubren de forma automática.

j) Seleccione o especifique el **Juego de caracteres del registro de alertas de Oracle**. Es la página de códigos de los archivos de registro de alertas correlacionados.

Si este parámetro está en blanco, se utiliza el valor de entorno local actual del sistema, por ejemplo:

- ISO8859_1, codificación de Europa occidental ISO 8859-1
- UTF-8, codificación UTF-8 de Unicode
- GB18030, codificación GB18030 de chino simplificado
- CP950, codificación de chino tradicional
- EUC_JP, codificación de japonés
- EUC_KR, codificación de coreano

Para obtener una lista completa de todas las páginas de códigos soportadas, consulte Páginas de códigos soportadas en ICU.

k) Pulse **Aplicar** para guardar los valores de la instancia de conexión de base de datos en la sección **Conexiones de base de datos**.

l) (Opcional) Probar la conexión de base de datos nueva.

1) Seleccione la conexión a base de datos nueva en la sección **Conexiones de base de datos**.

2) Pulse **Probar conexión**.

3) Observe los resultados en la ventana de resultados **Probar conexión**.

- Ejemplo de **Resultado de prueba** satisfactorio:

```
Testing connection config1 ...
Success
```

- Ejemplo de **Resultado de prueba** no satisfactorio:

```
Testing connection config1 ...
KBB_RAS1_LOG; Set MAXFILES to 1
ORA-12514: TNS:listener does not currently know of service requested in connect
descriptor
Failed
```

m) Pulse **Siguiente**.

6. Lea la información del panel **Resumen** de la ventana **Configurar ITCAM Extended Agent for Oracle Database** y pulse **Aceptar** para terminar la configuración de una instancia de agente.
7. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en **Monitoring Agent for Oracle Database** y luego pulse **Iniciar**.

Qué hacer a continuación

- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte “Inicio de la Consola de Cloud APM” en la página 1009.

Configuración del agente respondiendo a solicitudes

Para configurar el agente en sistemas operativos Linux y UNIX, ejecute el script de configuración de líneas de mandatos y responda a sus solicitudes.

Procedimiento

1. Abra el directorio *dir_instalación*/bin, donde *dir_instalación* es el directorio de instalación del Agente de Oracle Database.
2. (Opcional) Para listar los nombres de las instancias de agente configuradas, ejecute el mandato siguiente: **./cinfo -o rz**.
3. Para configurar el Agente de Oracle Database, ejecute el mandato siguiente: **./oracle_database-agent.sh config** *nombre_instancia*.
4. Cuando se le solicite `Editar 'valores del Monitoring Agent for Oracle Database'`, pulse **Intro**. El valor predeterminado es `Sí`.
5. Para especificar la información de `Configuración de base de datos predeterminada`, siga estos pasos:

   Nota: La sección `Configuración de base de datos predeterminada` no corresponde a la configuración de instancia de conexión de base de datos. Es una sección de la plantilla destinada a establecer lo que se utiliza como valores predeterminados al añadir las configuraciones de instancia de conexión de base de datos reales, que empiezan en el paso 6.

   a) Cuando se le solicite el `Nombre de usuario predeterminado`, especifique el ID de usuario de base de datos predeterminado para la conexión y pulse **Intro**.

   Este ID de usuario es el ID que el agente utiliza para acceder a la instancia de base de datos supervisada. Este ID de usuario debe tener privilegios de selección en las vistas y tablas de rendimiento dinámicas que son necesarias para el agente.

   b) Cuando se le solicite `Especificar contraseña predeterminada`, escriba la contraseña que está asociada con el ID de usuario de base de datos predeterminado especificado y pulse **Intro**. A continuación, confirme la contraseña si se le solicita.

   c) Si la versión del agente de Oracle es 8.0, realice este paso.

      1) Especifique el **`Archivo Jar JDBC de Oracle`**. Esta es la vía de acceso completa al archivo jar del controlador JDBC de Oracle utilizado para comunicarse con la base de datos Oracle. El controlador JDBC (Java Database Connectivity) de Oracle controlador que da soporte a las versiones de base de datos de Oracle supervisadas por el agente de Oracle debe estar disponible en el sistema del agente.

   d) Si la versión del agente de Oracle es 6.3.1.10, siga estos pasos.

      1) Cuando se le solicite el `Directorio inicial de Oracle`, si el Agente de Oracle Database está instalado en el servidor de bases de datos Oracle que se supervisa, especifique el directorio `inicial de Oracle` y pulse **Intro**. Si el Agente de Oracle Database no está instalado en el servidor de bases de datos Oracle que se va a supervisar, deje este valor en blanco, pulse **Intro** y ejecute el paso siguiente. Si desea borrar el valor del `Directorio inicial de Oracle`, pulse la barra espaciadora y, a continuación, pulse **Intro**.

         Nota: opcionalmente, para la supervisión local, el `Directorio inicial de Oracle` y el `Directorio de instalación del cliente de Oracle Instant` pueden dejarse en blanco para que se utilice la variable de entorno del sistema *ORACLE_HOME*.

      2) Si el Agente de Oracle Database es remoto con respecto al servidor de bases de datos Oracle que se supervisa, especifique el `Directorio de instalación del cliente de Oracle Instant` y pulse **Intro**. Si establece `Directorio inicial de Oracle` en el paso "5.d.i" en la página 644, este valor se ignora.

   e) `Directorios de archivos de configuración de red` puede dejarse en blanco para que se utilice el directorio predeterminado. Si la versión del agente de Oracle es 6.3.1.10, puede especificar varios directorios de archivos de configuración de red utilizando Windows ";" o

Linux AIX ":" para separar los directorios. En la versión del agente de Oracle 8.0, sólo se admite un directorio. Pulse **Intro**.

Este valor contiene el archivo o archivos de configuración de red de la base de datos Oracle. El directorio lo define la variable de entorno *TNS_ADMIN* para cada instancia de base de datos Oracle. El directorio predeterminado es Linux AIX `$ORACLE_HOME/network/admin` o Windows `%ORACLE_HOME%\NETWORK\ADMIN`. Si no se configura este valor, se utiliza el directorio predeterminado. Para inhabilitar el uso del directorio predeterminado, establezca la siguiente variable de entorno del agente en false: `KRZ_LOAD_ORACLE_NET=false`.

f) Elija si el escucha dinámico predeterminado está configurado en esta estación de trabajo y pulse **Intro**.

El escucha dinámico predeterminado es `(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)`. Si el escucha dinámico predeterminado está configurado en esta estación de trabajo, establezca este valor en True.

g) Deje el `Nombre de archivo de definición de SQL personalizado` en blanco. No se utiliza.

6. Se le solicitará `Editar valores de 'Conexión a base de datos'` tras visualizar la salida siguiente en la pantalla:

```
Configuración de instancia :
Resumen :
Conexión a base de datos :
```

Nota: Este es el paso en el que se definen las instancias de conexión a base de datos reales. Debe añadir como mínimo una. También aquí se editan y suprimen las instancias de conexión de base de datos. Si existen varias configuraciones de instancia de conexión a base de datos, utilice la opción `Siguiente` para pasar por alto las instancias que no deben editarse ni suprimirse hasta llegar a la instancia que debe editar o suprimir.

7. Para añadir una nueva conexión de base de datos, especifique 1 y pulse **Intro**.
8. Para especificar la información de conexión de base de datos, siga estos pasos:

a) Cuando se le solicite el `Nombre de conexión a base de datos`, especifique un alias para la conexión con la base de datos y pulse **Intro**.

Este alias puede ser cualquier cosa que elija para representar la conexión a base de datos, con las limitaciones siguientes. Sólo se pueden utilizar letras, números arábigos, el carácter de subrayado y el símbolo "menos" en el nombre de la conexión. La longitud máxima de un nombre de conexión son 25 caracteres.

b) Cuando se le solicite el `Tipo de conexión`, seleccione uno de los tipos siguientes de conexión:

1) (Opcional) Básica

El tipo de conexión predeterminado y más habitual es **Básica**. Si no está seguro del tipo de conexión necesario, es aconsejable elegir este tipo de conexión.

a) Seleccione el tipo de conexión **Básica** si la base de datos supervisada de destino es una sola instancia, como por ejemplo una instancia de sistema de archivos estándar o una sola instancia de ASM.

b) Cuando se le solicite el `Nombre de host`, escriba el nombre de host o la dirección IP para la base de datos Oracle y pulse **Intro**.

c) Cuando se le solicite el `Puerto`, escriba el número de puerto y pulse **Intro**.

d) Especifique uno de estos dos valores: `Nombre de servicio` o `SID`.

i. (Opcional) Cuando se le solicite el `Nombre de servicio`, escriba el nombre del servicio que es una representación lógica de una base de datos, una serie de caracteres que es el nombre del servicio de base de datos global, pulse **Intro** y continúe en el paso 8c.

Un nombre de servicio es una representación lógica de una base de datos, que es la forma en que la base de datos se presenta a los clientes. Una base de datos puede

presentarse en forma de varios servicios, y un servicio puede implementarse en forma de varias instancias de base de datos. El nombre de servicio es una serie que es el nombre de base de datos global, es decir, un nombre formado por el nombre de base de datos y el nombre de dominio, especificado durante la instalación o la creación de la base de datos. Si no está seguro de cuál es el nombre de base de datos global, puede obtenerlo a partir del valor del parámetro SERVICE_NAMES del archivo de parámetros de inicialización. Este parámetro se puede dejar en blanco si establece el SID en el paso "8.b.i.4.b" en la página 646.

ii. (Opcional) Cuando se le solicite el SID, escriba el identificador de sistema Oracle que identifica una instancia específica de una base de datos en ejecución, pulse **Intro** y continúe en el paso paso 8c.

Este parámetro es el identificador de sistema Oracle que identifica una instancia específica de una base de datos. Si se ha definido `Nombre de servicio` en el paso "8.b.i.4.a" en la página 645, puede dejar este elemento en blanco.

2) (Opcional) TNS

a) Seleccione el tipo de conexión **TNS** cuando se ha establecido la variable de entorno de sistema *ORACLE_HOME HOME* y el alias de TNS para la base de datos supervisada de destino está definido en el archivo `$ORACLE_HOME/network/admin/tnsnames.ora`.

b) Especifique el nombre de alias de TNS, pulse **Intro** y continúe en el paso 8c.

3) (Opcional) Avanzada

a) Seleccione el tipo de conexión **Avanzada** cuando hay más de una instancia de Oracle en varios nodos físicos para la base de datos de destino supervisada. Por ejemplo, una base de datos ASM con RAC (Real Applications Cluster).

b) Especifique la serie de conexión de Oracle, pulse **Intro** y continúe en el paso 8c.

Este atributo soporta todos los métodos de denominación de Oracle Net de la siguiente manera:

- Serie de URL de conexión SQL con el formato: `//host:puerto/nombre de servicio`. Por ejemplo, `//dlsun242:1521/bjava21`.
- Par palabra clave-valor de Oracle Net. Por ejemplo,

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=bjava21)))
```

- Entradas **TNSNAMES**, como por ejemplo **inst1,** con la variable de entorno *TNS_ADMIN* o *ORACLE_HOME* establecida y los archivos de configuración configurados.

Nota: la descripción que se muestra durante la configuración por línea de mandatos puede contener una barra inclinada invertida antes de los símbolos de dos puntos (\:) y de signo igual (\=). No especifique barras inclinadas invertidas en la serie de conexión. Se visualizan en la descripción para escapar del comportamiento normal de interpretar el signo igual como parte de un mandato, interpretándolo simplemente como texto.

c) Continúe en el paso 8c.

c) Cuando se le solicite el `Nombre de usuario de base de datos`, especifique el ID de usuario de base de datos para la conexión y pulse **Intro**.

Para instancias de sistema de archivos estándar, este ID de usuario debe tener privilegios de selección en las vistas y tablas de rendimiento dinámicas que son necesarias para el agente.

Para instancias de ASM, utilice una cuenta con el rol **SYSDBA** o **SYSASM**. Por ejemplo, la cuenta sys.

d) Cuando se le solicite `Especificar la contraseña de base de datos`, escriba la contraseña que está asociada con el ID de usuario de base de datos especificado.

e) Cuando se le solicite el `Rol`, elija el rol que coincida con los permisos otorgados al ID de usuario especificado y pulse **Intro**.

El rol es el conjunto de privilegios que deben asociarse con la conexión. Para un usuario con el privilegio del sistema SYSDBA, especifique un rol que incluya ese privilegio.

Para instancias de ASM, utilice el rol **SYSDBA** o **SYSASM**.

f) Cuando se le soliciten las `Vías de acceso del archivo de registro de alertas Oracle (incluidos los nombres de archivo de registros de alerta)`, especifique las vías de acceso de registro de alertas y pulse **Intro**.

Este parámetro corresponde a las vías de acceso de archivo absolutas de archivos de registro de alertas correlacionados para instancias de base de datos remotas en esta conexión de base de datos. El agente supervisa el registro de alertas leyendo estos archivos. Normalmente, se encuentran en $ORACLE_BASE/diag/rdbms/*NOMBRE_BD*/*SID*/trace/alert_*SID*.log. Por ejemplo si *DB_NAME* y *SID* son db11g, y *ORACLE_BASE* es /home/dbowner/app/oracle, el registro de alertas se encontrará en /home/dbowner/app/oracle/diag/rdbms/db11g/db11g/trace/alert_db11g.log.

Windows Si el Agente de Oracle Database se ejecuta y lee los archivos de registro de alertas a través de la red, la vía de acceso del archivo remoto debe cumplir los convenios de denominación universal de sistemas Windows. Por ejemplo, \\tivx015\path\alert_orcl.log.

Importante: Especifique la vía de acceso y el nombre del archivo de registro de alertas juntos. Una vía de acceso del registro de alertas no soporta el controlador de red correlacionado.

Linux AIX Si se ejecuta el Agente de Oracle Database, se necesita un sistema de archivos montado localmente para los registros de alertas remotas.

Windows Los diversos archivos se separan con un punto y coma (;).

Linux AIX Los diversos archivos se separan con dos puntos (:).

Cada archivo se compara con una instancia de base de datos mediante el patrón de nombre de archivo alert_*instancia*.log o, si no coincide, se ignora.

Los registros de alertas de la instancia de base de datos local se pueden descubrir de forma automática.

g) Cuando se le solicite el **Juego de caracteres de archivo de registro de alertas de Oracle**, especifique la página de códigos de los archivos de registro de alertas correlacionados y pulse **Intro**

Si este parámetro está en blanco, se utiliza el valor de entorno local actual del sistema, por ejemplo:

- ISO8859_1, codificación de Europa occidental ISO 8859-1
- UTF-8, codificación UTF-8 de Unicode
- GB18030, codificación GB18030 de chino simplificado
- CP950, codificación de chino tradicional
- EUC_JP, codificación de japonés
- EUC_KR, codificación de coreano

Para obtener una lista completa de todas las páginas de códigos soportadas, consulte Páginas de códigos soportadas en ICU.

9. Cuando se le solicite de nuevo `Editar valores de 'Conexión a base de datos'`, verá el nombre de la conexión a base de datos que ha establecido en el paso 8a. Puede volver a editarlo o suprimirlo. Si ya tiene configurada más de una instancia de conexión a base de datos, utilice **Siguiente** para recorrerlas.
10. (Opcional) Para añadir otra conexión de base de datos para supervisar varias instancias de base de datos con esta instancia de agente, especifique 1, pulse **Intro** y vuelva alPaso 8.
11. Cuando haya terminado de modificar las conexiones de base de datos, especifique 5 y pulse **Intro** para salir del proceso de configuración.

12. Para iniciar el agente, especifique:
    dir_instalación/bin/oracle_database-agent.sh start *nombre_instancia*.

Qué hacer a continuación

- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

1. Abra el archivo `oracle_silent_config.txt` en un editor de texto:
   - Linux AIX *dir_instalación*/samples/oracle_database_silent_config.txt.
   - Windows *dir_instalación*\samples\oracle_database_silent_config.txt
2. Para **Nombre de usuario predeterminado**, especifique el nombre del usuario de base de datos predeterminado para las conexiones de base de datos que crean para esta instancia de agente. Por ejemplo **KRZ_CONN_USERID=**usuario1.

   Nota: este usuario debe tener privilegios suficientes para completar las tareas que realiza este agente mientras está conectado a la base de datos, como por ejemplo consultar tablas.
3. Para **Contraseña predeterminada**, debe especificar la contraseña que está asociada con el usuario de base de datos predeterminado especificado. Por ejemplo, **KRZ_CONN_PASSWORD=**Contraseña.
4. Si la versión del agente de Oracle es 8.0, realice este paso.
   a) Especifique el **Archivo Jar JDBC de Oracle**. Esta es la vía de acceso completa al archivo jar del controlador JDBC de Oracle utilizado para comunicarse con la base de datos Oracle.

      El controlador JDBC (Java Database Connectivity) de Oracle controlador que da soporte a las versiones de base de datos de Oracle supervisadas por el agente de Oracle debe estar disponible en el sistema del agente.
5. Si la versión del agente de Oracle es 6.3.1.10, siga estos pasos.
   a) Si el Agente de Oracle Database está instalado en el servidor de bases de datos Oracle que se supervisa, especifique el directorio `inicial de Oracle`. Por ejemplo, **KRZ_ORACLE_HOME=**vía_acceso_inicio.

      Nota: en los parámetros opcionales como este, elimine el símbolo de almohadilla (#) inicial para poder utilizarlos.

      Si el Agente de Oracle Database no está instalado en el servidor de bases de datos Oracle que se va a supervisar, deje este valor en blanco y complete el paso siguiente.

      Nota: opcionalmente, para la supervisión local, el `Directorio inicial de Oracle` y el `Directorio de instalación del cliente de Oracle Instant` pueden dejarse en

blanco (comentarse con un símbolo de almohadilla (#) en la primera posición de la línea de parámetros del archivo de texto de configuración silenciosa), para que se utilice la variable de entorno del sistema *ORACLE_HOME*.

b) Si el Agente de Oracle Database es remoto con respecto al servidor de bases de datos Oracle que se supervisa, especifique el `Directorio de instalación del cliente de Oracle Instant`. Si ha especificado el `Directorio inicial de Oracle` en el paso anterior, este valor se ignorará.

- Windows Defina la vía de acceso de carpeta completa del directorio **`inicial de Oracle`** que contiene los archivos de biblioteca de `OCI (Oracle Call Interface)`. Si la vía de acceso completa del archivo `oci.dll` es `C:\instantclient_10_2\oci.dll`, debe definir esta vía de acceso `C:\instantclient_10_2`. Por ejemplo, **`KRZ_INSTANT_CLIENT_LIBPATH=`**`C:\instantclient_10_2`
- AIX Defina la vía de acceso de carpeta completa del directorio **`inicial de Oracle`** que contiene los archivos de biblioteca de `OCI (Oracle Call Interface)`. Si la vía de acceso completa del archivo `libocci.so.10.1` es `/home/tivoli/oci/libocci.so.10.1`, debe definir esta vía de acceso `home/tivoli/oci`. Por ejemplo, **`KRZ_INSTANT_CLIENT_LIBPATH=`**`/home/tivoli/oci`

6. `Directorios de archivos de configuración de red` puede dejarse en blanco para que se utilice el directorio predeterminado. El Agente de Oracle Database utiliza esta vía de acceso de archivo para obtener el archivo `tnsnames.ora`. Este directorio lo define la variable de entorno *TNS_ADMIN* para cada instancia de base de datos Oracle. El directorio predeterminado es Linux AIX `$ORACLE_HOME/network/admin` o Windows `%ORACLE_HOME%\NETWORK\ADMIN`. Si especifica este valor con varios directorios de archivos de configuración de red, utilice Windows ";" o Linux AIX ":" para separar los directorios.

   Si está supervisando bases de datos Oracle de forma remota, puede copiar los archivos de configuración de red del sistema remoto en el sistema donde está instalado el agente. Además, puede fusionar el contenido de los archivos de configuración de red del sistema remoto con los archivos de configuración de red del sistema donde está instalado el agente.

7. Para **`Escucha dinámico`**, compruebe si el escucha dinámico predeterminado está configurado. El escucha dinámico predeterminado es (PROTOCOL=TCP)(HOST=localhost)(PORT=1521). Si el escucha dinámico predeterminado está configurado, establezca este valor en TRUE tal como se muestra a continuación: **`KRZ_DYNAMIC_LISTENER=`**TRUE.

   Los valores válidos son TRUE y FALSE.

8. Deje el `Nombre de archivo de definición de SQL personalizado` en blanco. No se utiliza.
9. A partir de aquí, se definen las instancias de conexión a base de datos reales. Debe añadir como mínimo una. Las entradas de una instancia se suministran en el archivo `oracle_silent_config.txt` con el nombre de instancia *config1*. Si cambia el nombre de instancia, asegúrese de cambiar todas las referencias.

   Este alias puede ser cualquier cosa que elija para representar la conexión a base de datos, con las limitaciones siguientes. Sólo se pueden utilizar letras, números arábigos, el carácter de subrayado y el símbolo "menos" en el nombre de la conexión. La longitud máxima de un nombre de conexión son 25 caracteres.

10. Para **`Tipo de conexión`**, especifique uno de los siguientes tipos de conexión: **Básica**, **TNS** o **Avanzada**. Por ejemplo, **`KRZ_CONN_TYPE.config1=`**`Básica`.
11. Para el tipo de conexión que ha seleccionado en el paso anterior, especifique los parámetros necesarios:

    Básica

    - Para **`Nombre de host`**, especifique el nombre de host o la dirección IP de la base de datos Oracle, por ejemplo: **`KRZ_CONN_HOST.config1=`** `nombre_host`.
    - Para **`Puerto`**, especifique el puerto de escucha para la base de datos Oracle, por ejemplo: **`#KRZ_CONN_PORT.config1=`** 1521.

- Para **Nombre de servicio**, especifique la representación lógica de la base de datos utilizando una serie para el nombre de base de datos global, por ejemplo: **KRZ_CONN_SERVICE.config1=** `orcl`.

  Importante: si no define aquí el Nombre de servicio, debe especificar el Identificador del sistema (SID) Oracle.

  Para **Identificador de sistema Oracle (SID)**, especifique un SID que identifique una instancia específica de una base de datos en ejecución, por ejemplo: **KRZ_CONN_SID.config1=** `sid`.

TNS

Para **TNS alias**, especifique el nombre de alias de red del archivo `tnsnames.ora`. Por ejemplo, **KRZ_CONN_TNS.config1=** `tnsalias`.

Avanzada

Para **Serie de conexión de Oracle**, especifique la serie de conexión de base de datos para OCI. Por ejemplo, **KRZ_CONN_STR.config1=** `//host:port/service`

Esta serie da soporte a todos los métodos de denominación de Oracle Net tal como se muestra a continuación:

- Para una serie URL de SQL Connect:

```
//host:[puerto][/nombre de servicio]
```

- Para un par palabra clave-valor de Oracle Net:

```
"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=bjava21)))"
```

Esta serie también admite entradas **TNSNAMES**, por ejemplo, **inst1**, en las que se hayan establecido las variable de entorno *TNS_ADMIN* o *ORACLE_HOME* y se hayan configurado los archivos de configuración.

Importante: este atributo sólo es aplicable al tipo de conexión avanzada.

12. Para **Nombre de usuario de base de datos**, puede especificar el nombre del usuario de base de datos para la conexión, por ejemplo: **KRZ_CONN_USERID=**`UserID`.

    Este usuario debe tener privilegios suficientes para completar las tareas que el agente requiere mientras está conectado a la base de datos, por ejemplo, crear, editar y suprimir tablas.

    Si este campo está vacío, el agente utiliza el nombre de usuario predeterminado en la sección de configuración de base de datos predeterminada. Si **Nombre de usuario de base de datos** no se ha configurado, el nombre de usuario predeterminado se utiliza para esta conexión.
13. Para **Contraseña de base de datos**, puede especificar la contraseña que está asociada con el usuario de base de datos especificado, por ejemplo: **KRZ_CONN_PASSWORD=**`Contraseña`.

    Si este campo está vacío, el agente utiliza la contraseña predeterminada en la sección de configuración de base de datos predeterminada. Si **Contraseña de base de datos** no se ha configurado, la contraseña predeterminada se utiliza para esta conexión.
14. Para **Rol**, puede especificar el conjunto de privilegios que están asociados con la conexión, por ejemplo **KRZ_CONN_MODE.config1=**`DEFAULT`.

    Los valores válidos son *SYSDBA*, *SYSOPER*, *SYSASM* y *DEFAULT*.

    Para un usuario con el privilegio del sistema *SYSDBA*, puede especificar una conexión que incluya este privilegio. Si este elemento no está definido, puede asignar el rol *DEFAULT* al usuario.
15. Para **Vías de acceso del archivo de registro de alertas Oracle**, cuando se incluye el nombre de archivo de registro de alertas, puede especificar la vía de acceso de archivo absoluta de los archivos de registro de alertas correlacionados para las instancias de base de datos remota en esta conexión de base de datos. Por ejemplo, **KRZ_LOG_PATHS.config1=**`AlertLogPath`.

    Windows Utilice un punto y coma (;) para separar los diversos archivos.

Linux AIX Utilice dos puntos (:) para separar los diversos archivos.

Cada archivo se compara con una instancia de base de datos mediante el patrón de nombre de archivo `alert_`*`instancia`*`.log`. De forma alternativa, se ignora si no coincide.

Los archivos de `registro de alertas de instancia de base de datos local` se descubren automáticamente.

Si **Vías de acceso del archivo de registro de alertas Oracle** no se ha configurado, el `registro de alertas` no está disponible.

16. Para **Juego de caracteres del registro de alertas de Oracle**, puede especificar la página de códigos de los archivos de registro de alertas correlacionados. Por ejemplo, **KRZ_LOG_CHARSET.config1=** `JuegoCaracteres`

    Si este campo está vacío, se utiliza el valor de entorno local actual del sistema, como se muestra a continuación:

    ```
    ISO8859_1: ISO 8859-1 Western European encoding
    UTF-8: UTF-8 encoding of Unicode
    GB18030: Simplified Chinese GB18030 encoding
    CP950: Traditional Chinese encoding
    EUC_JP: Japanese encoding
    ```

17. Guarde y cierre el archivo `oracle_database_silent_config.txt`. A continuación, especifique: *`dir_instalación`*`/bin/oracle_database-agent.sh config` *`nombre_instancia`* *`dir_instalación`*`/samples/oracle_database_silent_config.txt`
    donde *`nombre_instancia`* es el nombre que desea proporcionar a la instancia.
18. Para iniciar el agente, especifique:
    `dir_instalación``/bin/oracle_database-agent.sh start` *`nombre_instancia`*.

Qué hacer a continuación

- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Otorgar privilegios al usuario del agente de la base de datos Oracle

Después de instalar el agente, debe otorgar privilegios a la cuenta de usuario de Oracle utilizado por el Agente de Oracle Database.

Puede otorgar privilegios para los usuarios siguientes:

- Usuarios de instancia de sistema de archivos estándar (no ASM)
- Usuarios de instancia de ASM con RAC no SYS

Cómo otorgar privilegios a usuarios para instancias de sistema de archivos estándar
Para instancias de sistema de archivos estándar, el ID de usuario de Oracle utilizado por el Agente de Oracle Database deberá tener privilegios de selección en la vistas de rendimiento dinámicas, tablas y vistas de diccionario de datos que necesite el agente. Deberá tener también otros privilegios de objeto de Oracle y del sistema que sean necesarios para ejecutar determinados mandatos de base de datos.

Procedimiento

1. (Opcional) Si un ID de usuario de la base de datos Oracle no existe, cree este ID utilizando los recursos de Oracle y ejecutando el mandato siguiente: `create user` *`NombreUsuario`* `identified by` *`Contraseña`*
2. Otorgue privilegios de selección para las vistas de rendimiento dinámicas, tablas y vistas de diccionario de datos al ID de usuario de Oracle que ha creado ejecutando el script **krzgrant.sql** suministrado con el Agente de Oracle Database. Este paso debe llevarse a cabo antes de configurar el agente. Para obtener instrucciones sobre cómo personalizar y ejecutar el script **krzgrant.sql**,

consulte “Personalización del script krzgrant.sql” en la página 652 y “Ejecución del script krzgrant.sql” en la página 653.

Nota: Los privilegios de selección para vistas de rendimiento dinámicas, tablas y vistas de diccionario de datos dependen de las prestaciones de la base de datos Oracle en entornos de aplicación específicos. Puede otorgar privilegios de Oracle autorizados al ID de usuario de base de datos Oracle sólo para las vistas de rendimiento dinámicas, tablas y vistas de diccionario de datos que utiliza el Agente de Oracle Database.

3. Otorgue privilegios de objeto de Oracle y privilegios del sistema al ID de usuario de Oracle utilizado por el Agente de Oracle Database utilizando los recursos de Oracle.

Personalización del script krzgrant.sql

Si no desea permitir privilegios de selección autorizados de Oracle en algunas vistas de rendimiento dinámicas, tablas y vistas de diccionario de datos en el script **krzgrant.sql**, puede personalizar el script **krzgrant.sql** antes de ejecutarlo.

Nota: La instancia de agente comprueba todos los privilegios predeterminados en el script **krzgrant.sql** y notifica un suceso de agente con una falta de privilegios cuando se inicia el agente. Puede inhabilitar la comprobación de privilegios utilizando el siguiente configuración de variable: KRZ_CHECK_ORACLE_PRIVILEGE=FALSE. El paso de conexión de prueba de la configuración de GUI comprueba todos los privilegios de Oracle definidos en el archivo `krzgrant.sql`. Si confirma que el usuario de Oracle tiene los privilegios correctos, ignore que la comprobación de privilegios falle en el paso de conexión de prueba.

Edite el archivo `krzgrant.sql` en un editor de texto plano para eliminar o añadir el prefijo '--' al principio de las sentencias de otorgamiento a fin de saltarse la ejecución de otorgamiento para estas vistas o tablas de Oracle no autorizadas.

Por ejemplo, cambie las líneas siguientes:

```
    execute immediate 'grant select on DBA_HIST_SNAPSHOT to '||userName;
    execute immediate 'grant select on DBA_HIST_SQLSTAT to '||userName;
    execute immediate 'grant select on DBA_HIST_SQLTEXT to '||userName;
    execute immediate 'grant select on DBA_HIST_SQL_PLAN to '||userName;
    execute immediate 'grant select on DBA_HIST_SYSMETRIC_SUMMARY to '||userName;
```

por estas líneas:

```
--    execute immediate 'grant select on DBA_HIST_SNAPSHOT to '||userName;
--    execute immediate 'grant select on DBA_HIST_SQLSTAT to '||userName;
--    execute immediate 'grant select on DBA_HIST_SQLTEXT to '||userName;
--    execute immediate 'grant select on DBA_HIST_SQL_PLAN to '||userName;
--    execute immediate 'grant select on DBA_HIST_SYSMETRIC_SUMMARY to '||userName;
```

Cómo otorgar privilegios a usuarios no SYS para instancias de ASM

Debe conectarse a las instancias de ASM que utilizan los usuarios con roles SYSDBA y SYSASM. Si no necesita utilizar la cuenta SYS para conectarse a instancias de ASM, cree una cuenta de usuario y otorgue a dicha cuenta los roles SYSDBA y SYSASM.

Procedimiento

1. Ejecute los mandatos siguientes para crear una cuenta de usuario y otorgar roles:
   - Inicie la sesión en una base de datos de ASM con el rol SYSASM para crear un nuevo usuario para un agente y otorgar el rol SYSDBA o SYSASM:
     a.
     ```
     create user NombreUsuario identified by
     contraseña
     ```
     b.
     ```
     grant sysdba to NombreUsuario
     ```
     o bien
     ```
     grant sysasm to NombreUsuario
     ```

2. Al crear la conexión de ASM en la ventana de configuración, especifique el usuario *NombreUsuario* y el rol SYSDBA o SYSASM.

   Nota: Si elige el rol SYSASM para acceder a la base de datos ASM, debe configurar la instancia de agente utilizando el inicio de Oracle o el cliente instantáneo de Oracle para conectarse a la base de datos Oracle.

Ejecución del script krzgrant.sql

Antes de empezar

- Si no ejecuta el script **krzgrant.sql**, surge un suceso en el espacio de trabajo de sucesos del agente.
- Para completar el procedimiento de instalación, consulte Capítulo 6, “Instalación de los agentes”, en la página 125.

Después de la instalación, podrá buscar el script **krzgrant.sql** en el directorio siguiente:

- Windows *dir_instalación*\TMAITM6_X64
- Linux AIX *dir_instalación*/*architecture*/rz/bin

donde:

dir_instalación
Directorio de instalación del Agente de Oracle Database.

arquitectura
Identificador de la arquitectura del sistema IBM Application Performance Management o Cloud APM. Por ejemplo, lx8266 representa Linux Intel v2.6 (64 bits). Para obtener una lista completa de los códigos de arquitectura, consulte el archivo *dir_instalación*/registry/archdsc.tbl.

El script **krzgrant.sql** se usa con la sintaxis siguiente: krzgrant.sql *ID_usuario directorio_temporal*

donde:

ID_usuario
El ID del usuario de Oracle. Este ID de usuario se debe crear antes de ejecutar este archivo SQL. Valor de ejemplo: *tivoli*.

directorio_temporal
El nombre del directorio temporal que contiene el archivo de salida krzagent.log del script **krzgrant.sql**. El directorio debe existir antes de ejecutar este script SQL. Valor de ejemplo: dir_instalación/tmp.

Debe tener el rol de autorización de administrador de base de datos (DBA) de Oracle así como permiso de escritura en el directorio temporal para realizar el siguiente procedimiento.

Procedimiento

1. En la línea de mandatos, ejecute los mandatos para establecer las variables de entorno.
   - Windows

     ```
     SET ORACLE_SID= sid
     SET ORACLE_HOME= inicio
     ```

   - Linux AIX

     ```
     ORACLE_SID = sid
     export ORACLE_SID
     ORACLE_HOME = inicio
     export ORACLE_HOME
     ```

   donde:

sid
Identificador del sistema de Oracle, que diferencia entre mayúsculas y minúsculas.

inicio
Directorio de inicio de la instancia de Oracle supervisada.

2. Desde la misma ventana de la línea de mandatos donde establece variables de entorno, inicie Oracle SQL Plus o una herramienta alternativa que utilice para emitir sentencias SQL.
3. Inicie la sesión en la base de datos de Oracle como un usuario con privilegios de DBA (administrador de base de datos) en Oracle.
4. Vaya al directorio que contiene el script **`krzgrant.sql`** y ejecute el mandato siguiente para otorgar privilegios de selección:

```
@krzgrant.sql ID_usuario directorio_temporal
```

La salida se registra en el archivos `krzagent.log` del directorio temporal. Este registro almacena las vistas y las tablas para las que se otorgan privilegios de selección al Agente de Oracle Database.

Cuando se hayan otorgado los privilegios satisfactoriamente, ya se podrá configurar e iniciar el Agente de Oracle Database.

Configuración de la supervisión del sistema operativo

Los agentes de Monitoring Agent for Linux OS, Monitoring Agent for UNIX OS y Monitoring Agent for Windows OS se configuran automáticamente. Puede configurar la supervisión de archivos de registro para los agentes de sistema operativo con el fin de poder supervisar los archivos de registro de aplicación. Puede ejecutar los agentes de sistema operativo como usuario no root. También hay algunas opciones de configuración adicionales para el agente de sistema operativo Linux.

Ejecución de agentes de sistema operativo como un usuario no root

Puede ejecutar Monitoring Agent for Windows OS, Monitoring Agent for UNIX OS y Monitoring Agent for Linux OS como un usuario no root.

Para ejecutar Agente de sistema operativo Windows como un usuario no root, consulte “Ejecución de Monitoring Agent for Windows OS como usuario no root” en la página 655.

Para ejecutar agentes de Monitoring Agent for UNIX OS y Monitoring Agent for Linux OS como un usuario no root, consulte “Inicio de agentes mediante un usuario no root” en la página 1047.

Restricción:

Durante la ejecución como usuario no root, el agente no puede acceder a `/proc/pid/status`, y por tanto, no puede comunicar los siguientes atributos:

- -Tiempo de CPU de usuario (UNIXPS.USERTIME)
- -Tiempo de CPU del sistema (UNIXPS.SYSTEMTIM)
- -Tiempo total de CPU (UNIXPS.TOTALTIME)
- -Recuento de hebras (UNIXPS.THREADCNT)
- -Tiempo de CPU de usuario hija (UNIXPS.CHILDUTIME)
- -Tiempo de CPU de sistema hija (UNIXPS.CHILDSTIME)
- -Tiempo total de CPU hija (UNIXPS.CHILDTIME)
- -Tiempo de espera de CPU (UNIXPS.WAITCPUTIM)
- -Terminal (UNIXPS.USERTTY)

Estos atributos no son visibles en la Consola de Cloud APM, pero están disponibles para crear umbrales.

Ejecución de Monitoring Agent for Windows OS como usuario no root

Puede ejecutar Agente de sistema operativo Windows como usuario no root. Sin embargo, algunas funciones no están disponibles.

Al ejecutar Agente de sistema operativo Windows como usuario no root, algunas funciones no están disponibles en los siguientes grupos de atributos, si son propiedad únicamente de la cuenta de administrador:

- Registro
- Tendencia de archivo
- Cambio de archivo

El despliegue remoto de otros a agentes no está disponible porque se necesitan derechos de administrador para instalar agentes nuevos.

Para los Servicios de gestión de agentes, el proceso de vigilancia no puede detener ni iniciar aquellos agentes para los que no tenga privilegios de detener o iniciar.

Para crear un usuario no root, cree un nuevo usuario limitado (no root) y configure los permisos del registro para el nuevo usuario como en el siguiente ejemplo:

- Acceso completo a `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`
- Acceso de lectura a `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Perflib`

El usuario que inicia el servicio Monitoring Agent for Windows OS – Primario debe tener derechos para gestionar el servicio Monitoring Agent for Windows OS - Proceso de vigilancia. El usuario que inicia el servicio Monitoring Agent for Windows OS - Proceso de vigilancia también debe tener derechos para gestionar todos los servicios gestionados por los Servicios de gestión de agente, incluido el servicio Monitoring Agent for Windows OS – Primario. Para otorgar a los usuarios la autorización para gestionar servicios del sistema en Windows, utilice plantillas de seguridad, política de grupos o edite el archivo `Subinacl.exe`. Para más información, consulte la siguiente documentación de Microsoft: http://support.microsoft.com/kb/325349(http://support.microsoft.com/kb/325349).

El siguiente ejemplo muestra cómo otorgar a los usuarios la autorización para gestionar servicios del sistema utilizando plantillas de seguridad:

1. Pulse **Inicio** > **Ejecutar**, escriba `mmc` en el recuadro Abrir y, a continuación, pulse **Aceptar**.
2. En el menú **Archivo**, pulse **Agregar o quitar complemento**.
3. Pulse **Añadir** > **Configuración y análisis de seguridad** y luego vuelva a pulsar **Añadir**.
4. Pulse **Cerrar** y a continuación pulse **Aceptar**.
5. En el árbol de consola, pulse con el botón del ratón en **Configuración y análisis de seguridad** y luego pulse **Abrir base de datos**.
6. Especifique un nombre y una ubicación para la base de datos y pulse **Abrir**.
7. En el recuadro de diálogo **Importar plantilla** que se visualiza, pulse la plantilla de seguridad que desea importar y pulse **Abrir**.
8. En el árbol de consola, pulse con el botón derecho del ratón en **Configuración y análisis de seguridad** y pulse **Analizar el equipo ahora**.
9. En el recuadro de diálogo **Realizar análisis** que se visualiza, acepte la vía de acceso predeterminada para el archivo de registro que se visualiza en el recuadro de vía de acceso del archivo de registro de errores. De lo contrario, especifique la ubicación que desea. Pulse **Aceptar**.
10. Cuando el análisis haya finalizado, configure los permisos del servicio como se indica a continuación:
    a. En el árbol de consola, pulse **Servicios del sistema**.
    b. En el panel derecho, haga una doble pulsación en el servicio Monitoring Agent for Windows OS - Primario.

c. Marque el recuadro de selección **Definir esta directiva en la base de datos** y, a continuación, pulse **Editar seguridad**.

d. Para configurar los permisos de un nuevo usuario o grupo, pulse **Agregar**.

e. En el recuadro de diálogo **Seleccionar usuarios, equipos o grupos**, escriba el nombre del usuario o grupo para el que desea establecer permisos y luego pulse **Aceptar**. En la lista **Permisos para usuario o grupo**, seleccione el recuadro de selección **Permitir** (situado junto a **Iniciar**). El permiso para detener y poner en pausa está seleccionado de forma predeterminada, de modo que el usuario o el grupo puede iniciar, detener y poner en pausa el servicio.

f. Pulse dos veces **Aceptar**.

11. Repita el paso 10 para configurar los permisos del servicio para el servicio Monitoring Agent for Windows OS - Proceso de vigilancia.
12. Para aplicar los nuevos valores de seguridad en el sistema local, pulse con el botón derecho del ratón en **Configuración y análisis de seguridad** y pulse **Configurar el equipo ahora**.

Nota: También puede utilizar la herramienta de línea de mandatos Secedit para configurar y analizar la seguridad del sistema. Para más información sobre Secedit, pulse **Inicio** > **Ejecutar**, escriba `cmd` y luego pulse **Aceptar**. En el indicador de mandatos, escriba `secedit /?` y pulse **INTRO**. Cuando utilice este método para aplicar configuraciones, se vuelven a aplicar todos los valores de la plantilla. Este método puede alterar temporalmente otros permisos de servicio, registro o archivo configurados anteriormente.

El siguiente ejemplo muestra cómo establecer los servicios Monitoring Agent for Windows OS y Proceso de vigilancia para iniciar la sesión como usuario no root utilizando la consola de servicios Windows:

1. Pulse **Inicio** > **Ejecutar**, escriba `services.msc` y luego pulse **Aceptar**.
2. Seleccione **Monitoring Agent for Windows SO - Primario**.
3. Pulse con el botón derecho del ratón en **Propiedades**.
4. Compruebe que el tipo de inicio sea Automático.
5. Seleccione la pestaña **Iniciar sesión** y, a continuación, seleccione **Iniciar sesión como "Esta cuenta"** y especifique el ID y la contraseña. Pulse **Aceptar**.
6. Seleccione **Monitoring Agent for Windows OS - Proceso de vigilancia**.
7. Pulse con el botón derecho del ratón en **Propiedades**.
8. Compruebe que el tipo de inicio sea Manual.
9. Seleccione la pestaña **Iniciar sesión** y, a continuación, seleccione **Iniciar sesión como "Esta cuenta"** y especifique el ID y la contraseña. Pulse **Aceptar**.

Configuración de la supervisión de archivos de registro del agente de sistema operativo

Los agentes de Monitoring Agent for Linux OS, Monitoring Agent for UNIX OS y Monitoring Agent for Windows OS se configuran automáticamente. Sin embargo, puede configurar la supervisión de archivos de registro para los agentes de sistema operativo, para que pueda supervisar los archivos de registro de la aplicación.

Después de que los agentes filtren los datos de registro, los datos se envían en forma de un suceso de registro a la Consola de Cloud APM.

Adición o eliminación de la configuración de supervisión de archivos de registro para los agentes de sistema operativo

Puede añadir una configuración de supervisión del archivo de registro para los agentes de sistema operativo para que estos agentes puedan filtrar los datos del archivo de registro. A continuación, posteriormente, puede eliminar también la configuración de la supervisión de archivos de registro para los agentes de sistema operativo, si es necesario.

Antes de empezar

Los agentes de sistema operativo incluyen ahora un archivo regex1.conf y un archivo regex1.fmt de ejemplo que puede ver antes de configurar los archivos .conf y .fmt. Los archivos están ubicados aquí:

- En UNIX/LINUX: `<dir_instalación>/samples/logfile-monitoring`
- En Windows: `<dir_instalación\samples\logfile-monitoring`

Utilice un editor de texto para crear archivo de configuración `.conf` y un archivo de formato `.fmt`. Para obtener más información sobre el contenido de estos archivos, consulte "Archivo de configuración" en la página 661 y "Archivo de formato " en la página 671. Debe asegurarse de guardar estos archivos en el sistema en el que accede a la consola de Performance Management, de forma que pueda cargar los archivos en el Servidor de Cloud APM.

Acerca de esta tarea

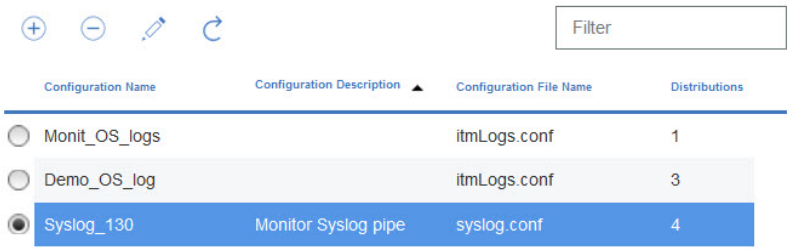
Para habilitar a los agentes de sistema operativo para que puedan supervisar archivos de registro, debe subir el archivo de configuración y el archivo de formato, y especificar a qué agente de sistema operativo se aplica la configuración. El agente de sistema operativo descarga los archivos `.conf` y `.fmt` y el agente supervisa los archivos de registro que se especifican en la configuración.

Procedimiento

Adición de la configuración de supervisión de archivos de registro para los agentes de sistema operativo

1. Pulse **Configuración del sistema** > **Configuración del agente**.
2. Según el sistema en el que desee supervisar los archivos de registro, pulse la pestaña **Sistema operativo Unix**, **Sistema operativo Linux** o **Sistema operativo Windows**.
3. Para crear una nueva configuración, pulse el icono (+) para abrir la ventana **Nueva configuración del archivo de registro**. Escriba un nombre para la configuración y una descripción de la configuración.
4. Para ver el contenido de los archivos `.conf` y `.fmt` archivos, pulse **Ver**.
5. Para cargar la configuración utilizando el Servidor de Cloud APM, seleccione el archivo `.conf` y el archivo `.fmt` desde el mismo sistema donde abre la consola de Performance Management y pulse **Terminado**.
6. En la pestaña del agente de sistema operativo, seleccione la configuración que ha subido.

   Importante: Los archivos `.conf` y `.fmt` que se distribuyen a los agentes se renombran por el nombre de configuración que defina.



7. Para desplegar la configuración, en la tabla **Lista de distribución de configuración de registro**, seleccione los agentes donde desea desplegar la configuración y pulse **Aplicar cambios**.

Eliminación de la configuración de supervisión de archivos de registro para los agentes de sistema operativo

8. Seleccione el nombre de la configuración.
9. Borre los sistemas gestionados y pulse **Aplicar cambios**.

   Importante:

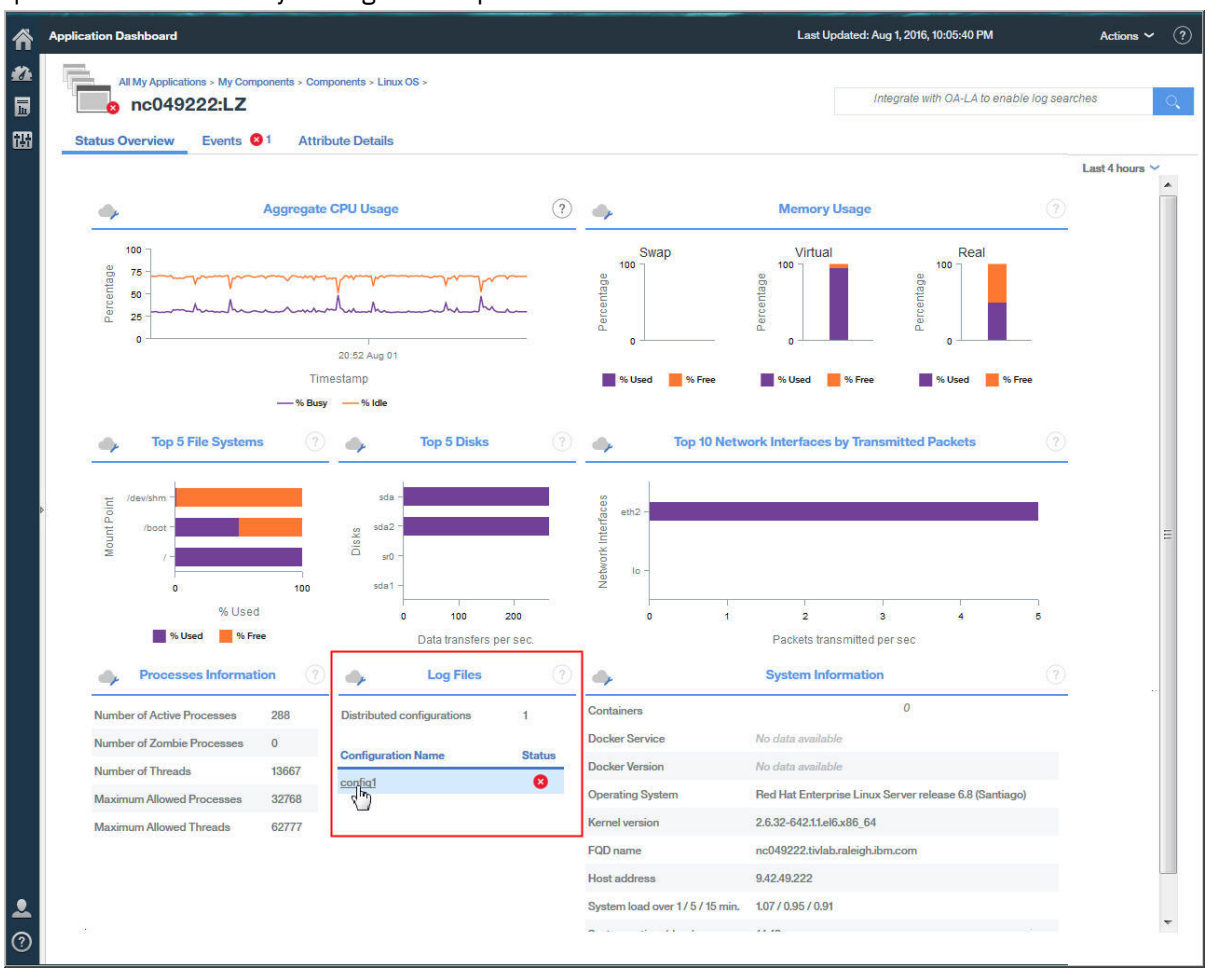
   Una vez eliminada la configuración de supervisión de archivos de registro, el recurso de supervisión de archivos de registro se mantiene y permanece en línea hasta que se reinicia el agente de sistema operativo. Los recursos de supervisión de archivos de registro fuera de línea se borran una vez que ha transcurrido el tiempo especificado en la opción **Eliminar retardo de sistema fuera de línea**.

Ver el contenido de supervisión del archivo de registro

Puede ver la configuración de supervisión del archivo de registro para los agentes de sistema operativo que ha desplegado para supervisar archivos de registro.

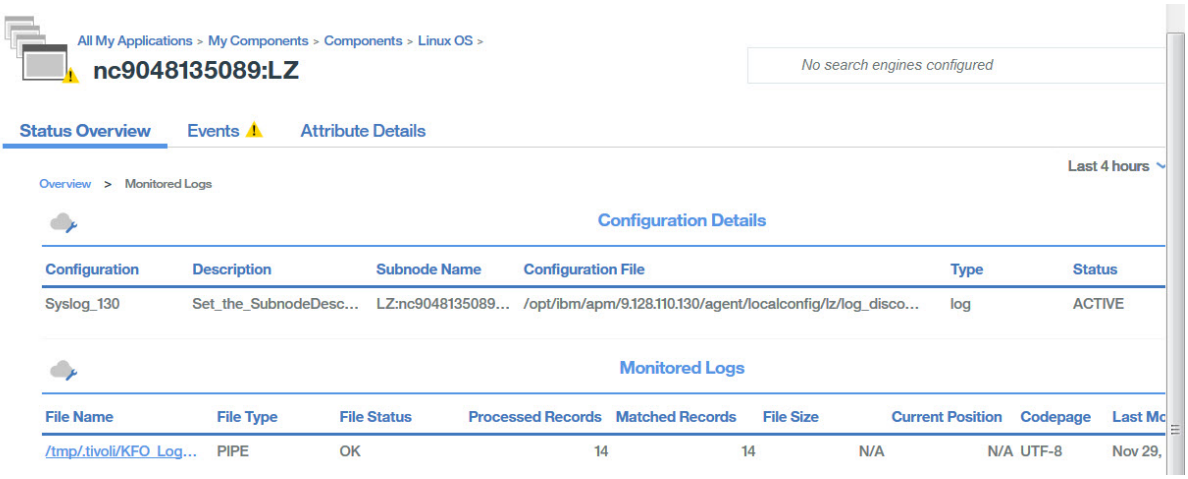
Procedimiento

1. Pulse **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** y seleccione una aplicación que incluya el agente de sistema operativo donde ha desplegado la configuración de supervisión del archivo de registro.
2. Descienda a un mayor nivel de detalle en el panel de instrumentos del agente de sistema operativo y, en el widget Archivos de registro, pulse el perfil para ver las configuraciones de supervisión de registro que se han distribuido y los registros supervisados.

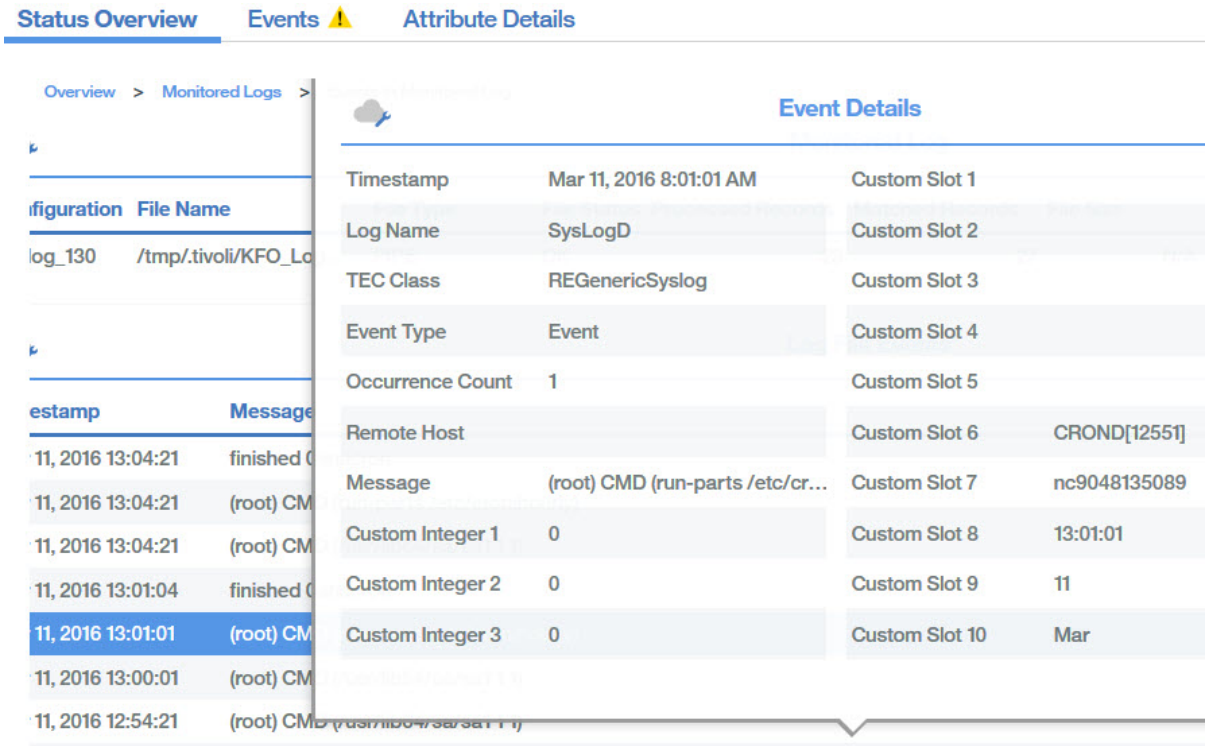


Los detalles de configuración incluyen nombre de configuración, descripción, subnodo, archivo de configuración, estado y código de error.

3. Pulse el nombre de archivo de registro para ver todos los sucesos del archivo de registro asociado con el archivo de registro.



4. Pulse en el suceso para ver los detalles del suceso, por ejemplo, todos los campos que ha definido en el archivo de formato.



Visualización de suceso de supervisión de archivo de registro
Después de configurar el agente de SO para supervisar los archivos de registro de la aplicación, puede crear nuevos umbrales para activar alarmas sobre las condiciones de las que desea que se le avise.

Procedimiento

1. En la barra de navegación, pulse **Configuración del sistema** > **Gestor de umbrales**.
2. Seleccione el sistema operativo de destino para **Tipo de origen de datos**.
3. Pulse Añadir para crear un nuevo umbral.
4. Establezca una gravedad para el suceso que supera este umbral.
5. Seleccione el conjunto de datos para el que desea crear un umbral. Los conjuntos de datos siguientes son elegibles para la supervisión de archivo de registro:
   - K*pp* Estadísticas de RegEx de archivo de registro
   - K*pp* Estado de archivo de registro

- K*pp* Sucesos de perfil de archivo de registro

6. Pulse **Añadir** para añadir una condición. En el recuadro **Añadir condición**, seleccione un atributo y un operador y, a continuación, especifique un valor de umbral.

   Repita este paso para añadir más condiciones al umbral si es necesario.
7. En la sección Asignación de grupos, seleccione el grupo de recursos al que desea asignar el umbral.
8. Pulse **Guardar**.
9. En la barra de navegación, pulse **Configuración del sistema** > **Configuración avanzada**.
10. En la categoría **Integración de interfaz de usuario**, establezca el valor de **Habilitar sucesos de subnodo** en True.
11. Pulse **Guardar**.

Resultados
Cuando la condición especificada sea verdadera, el suceso de archivo de registro que desencadena la alerta se mostrará en la pestaña Sucesos.

Variables de entorno de supervisión del archivo de registro
Puede establecer las variables de entorno para la supervisión de archivos de registro en los archivos de entorno de agente de sistema operativo.

Establezca las siguientes variables de entorno y sustituya K*PC* con el código de agente de sistema operativo donde *PC* es el código de agente de dos caracteres, por ejemplo, klz es el código para el agente del sistema operativo Linux.

K*PC*_FCP_LOG
Esta variable está disponible en el archivo *dir_instalación*/config/.*pc*.environment. El valor predeterminado es True y se utiliza para habilitar o inhabilitar la característica de supervisión de registro.

K*PC*_FCP_LOG_PROCESS_MAX_CPU_PCT
Este valor es el porcentaje máximo permitido de todas las CPU del sistema que el agente utiliza durante un intervalo de 1 minuto. Los valores válidos son del 5 al 100. El valor predeterminado es 100. Este valor está asociado con la característica de regulación de CPU. Si especifica un valor inferior a 5, se utiliza el valor mínimo 5.

K*PC*_FCP_LOG_PROCESS_PRIORITY_CLASS
Este valor es la prioridad del planificador del sistema operativo para el proceso. A es la prioridad más baja, C es el valor predeterminado del sistema operativo y F es la prioridad más alta. El valor es uno de los siguientes valores: A, B, C, D, E, F. Estos valores se reemplazan por todos los valores especificados en el archivo .conf.

K*PC*_FCP_LOG_SEND_EVENTS
El valor predeterminado es True y lo utiliza el agente del sistema operativo para enviar sucesos a Servidor de Cloud APM.

K*PC*_FCP_LOG_SEND_EIF_EVENTS
El valor predeterminado es True. Si esta opción se establece en Yes el agente envía los datos de sucesos a Servidor de Cloud APM o a cualquier receptor EIF como por ejemplo el analizador de EIF OMNIbus. Si la opción se establece en No, el agente no envía los datos de sucesos. El valor de esta opción es global y se aplica a todos los perfiles de supervisión.

Nota: El receptor EIF consume sucesos, de lo contrario se pueden producir problemas cuando la memoria caché del agente se llena.

K*PC*_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN
Los agentes del sistema operativo con supervisión de sucesos de archivo de registro tienen una limitación de subnodo. Para gestionar sucesos de archivo de registro, el MSN de subnodo tiene la siguiente estructura: UX:*CITRAHOSTNAME_PROFILENAME*. La limitación de tamaño máximo para el nombre de subnodo es de 32 caracteres. Si el nombre MSN de subnodo creado es demasiado largo y tiene más de 32 caracteres, se trunca en 32 caracteres. Este nombre corresponde a la subserie que se obtiene del nombre de perfil.

En el archivo de configuración del agente del sistema operativo, utilice las variables siguientes para gestionar los nombres de perfil que son demasiado largos:

- UNIX OS Agent: KUX_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true
- Linux OS Agent: KLZ_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true
- Windows OS Agent: KNT_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true

Por ejemplo, si tiene un agente que se denomina `aixhost_nc123456789A`, con una longitud de 20 caracteres, `CTIRAHOSTNAME=aixhost_nc123456789A` tiene 20 caracteres.

y tiene dos perfiles que se llaman:

```
ProfileLong12A (14 caracteres)
ProfileLong12B (14 caracteres)
```

se espera los siguientes MSN de subnodo relacionados:

```
UX:aixhost_nc123456789A_ProfileLong12A (38 caracteres)
UX:aixhost_nc123456789A_ProfileLong12B (38 caracteres)
```

Sin embargo, los MSN de subnodos se truncan en el límite de 32 caracteres de modo que los nombres resultantes es el mismo para ambos:

```
UX:aixhost_nc123456789A_ProfileL
UX:aixhost_nc123456789A_ProfileL
```

Para truncar CTIRAHOSTNAME en lugar del nombre de perfil, establezca la variable *Kpc_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true*.

Por ejemplo, si *n* es la longitud del nombre de perfil, como por ejemplo 14, la subserie para el nombre de MSN relacionado con *CTIRAHOSTNAME* se trunca en 32-n-3 caracteres, de modo que la variable *CTIRAHOSTNAME* es: `aixhost_nc1234`. A continuación, los MSN de subnodo distinguido son:

```
UX:aixhost_nc1234_ProfileLong12A
UX:aixhost_nc1234_ProfileLong12B
```

Archivo de configuración
Los agentes de sistema operativo utilizan un archivo de configuración que el agente lee cuando se inicia. El archivo contiene filtros y opciones de configuración. Debe crear este archivo de configuración y configurar la instancia del agente para utilizarlo.

El archivo de configuración se supervisa para determinar si hay cambios en su indicación de fecha y hora cada 60 segundos a partir de entonces. Si se modifica la indicación de fecha y hora del archivo, el agente reinicializa su configuración dinámicamente, sin necesidad de un reinicio. Para obtener más información, consulte “Modificación de los archivos de configuración de agente y de formato” en la página 674.

El archivo `.conf` para el agente del sistema operativo acepta estas opciones:

codepage
Este parámetro es la página de códigos del archivo supervisado. Utilice este parámetro en el archivo de configuración cuando la página de códigos del archivo supervisado es distinta de la página de códigos del sistema. Especifique la página de códigos del archivo supervisado, por ejemplo, ibm-5348_P100-1997, UTF-16 o UTF-8.

ConfigFilesAreUTF8=Y
Este parámetro especifica que el archivo de configuración y el archivo de formato están en UTF-8. Utilice este parámetro si la codificación de los archivos de configuración es UTF-8 y la página de código del sistema no lo es. El valor predeterminado es que el agente asume la codificación del sistema.

DupDetectionKeyAttributes
Una lista separada por comas de atributos de Cloud APM que se utiliza para determinar qué sucesos son duplicados. Si todos los atributos con nombre son iguales en dos sucesos, estos dos sucesos se

considerarán duplicados. Esta opción sólo es aplicable a los sucesos. Para obtener más información, consulte "Filtrado y resumen de sucesos" en la página 1052.

Nota:

1. Los nombres de atributos son sensibles a las mayúsculas y minúsculas, por lo que debe especificar los nombres exactamente a como se describen.
2. Si no se proporciona una lista de atributos, los valores predeterminados serán `Class` y `Logname`.

ENFORCE_STRICT_TEC_COMPATIBILITY
Este parámetro hace referencia a todos los caracteres de espacio en blanco en los datos de registro para asegurarse de que los caracteres son respetados. Por ejemplo, cuando se utiliza un formato como `"%s %s"` para extraer información de mensajes de registro, el agente de sistema operativo no sólo coincide con un espacio literal, sino también con los otros caracteres de espacio en blanco que están presentes, como pestañas y retornos de carro.

Cuando este parámetro no está establecido, el comportamiento predeterminado del agente de sistema operativo cuando coincide con una serie de formato de estilo de Tivoli Enterprise Console es hacer que coincida el máximo posible del texto de entrada, mientras procesa el formato de izquierda a derecha.

Por ejemplo, para la serie de formato `%s:%s` y la serie de entrada `one:two:three`, el valor predeterminado del agente del sistema operativo asigna `one.two` al primer parámetro (correspondiente al primer `%s`) y asigna `three` al segundo parámetro.

Nota:

1. Este parámetro no se aplica a sentencias de formato que utilicen la sintaxis de expresión regular.
2. El establecimiento de este parámetro afecta al rendimiento. Para obtener mayor control sobre el comportamiento y el rendimiento de las coincidencias, evite establecer este parámetro y, en su lugar, utilice expresiones regulares.

EventSummaryInterval
Especifica el número de segundos durante los cuales el agente busca sucesos duplicados a suprimir. Establezca este parámetro en un entero positivo. Esta opción sólo es aplicable a los sucesos. Para obtener más información, consulte "Filtrado y resumen de sucesos" en la página 1052.

EventFloodThreshold
Especifica qué sucesos se envían cuando se detectan sucesos duplicados. Establezca este parámetro en `send_none`, `send_all`, `send_first` o un entero positivo. Esta opción sólo es aplicable a los sucesos. Para obtener más información, consulte "Filtrado y resumen de sucesos" en la página 1052.

EventMaxSize
Especifica el tamaño máximo en bytes de un suceso generado. Si se especifica, este parámetro se utilizará en dos sitios:

1. El parámetro puede utilizarlo el agente para establecer el tamaño de un almacenamiento intermedio utilizado para procesar sucesos. Si no se establece, este almacenamiento intermedio tomará el tamaño predeterminado de 16384 bytes. Si el almacenamiento intermedio se establece demasiado pequeño, los sucesos se truncarán y se podrán descartar.
2. El parámetro puede utilizarlo el emisor EIF para establecer el tamaño de un almacenamiento intermedio utilizado para enviar sucesos a un receptor EIF, como el analizador de EIF OMNIbus. Si no se establece, este almacenamiento intermedio tomará el tamaño predeterminado de 4096 bytes. Si el almacenamiento intermedio se establece demasiado pequeño, se descartarán sucesos.

FileComparisonMode
Especifica qué archivos de registro se supervisarán cuando más de un archivo coincida con un patrón de comodín. Están disponibles los valores siguientes:

CompareByAllMatches
Este valor es el comportamiento predeterminado. Se supervisarán todos los archivos que coincidan con el patrón de comodín especificado en `LogSources`.

CompareByLastUpdate
De los archivos que coincidan con el patrón de comodín que se especifica en LogSources, se supervisa el archivo con la indicación de fecha y hora de actualización más reciente.

CompareBySize
De los dos o más archivos que coincidan con los criterios del patrón de nombre de archivo, se seleccionará el archivo más grande para la supervisión. No utilice CompareBySize con varios archivos coincidentes que se actualicen al mismo tiempo y aumenten su tamaño de archivo. Si el archivo más grande está sujeto a cambios frecuentes, la supervisión podría reiniciarse continuamente al principio del archivo recién seleccionado. En su lugar, utilice CompareBySize para un conjunto de archivos coincidentes donde sólo uno está activo y actualizándose en un determinado momento.

CompareByCreationTime
De los archivos que coincidan con el patrón de comodín que se especifica en LogSources, se supervisa el archivo con la indicación de fecha y hora de creada más recientemente. Este valor tiene las siguientes restricciones:

- El valor es aplicable solamente en sistemas operativos Windows porque los sistemas operativos UNIX y Linux no almacenan una hora de creación verdadera para los archivos.
- El valor no está soportado para archivos remotos que se supervisan utilizando FTP (File Transfer Protocol) de shell seguro (SSH).

Consejo: Los valores CompareByLastUpdate, CompareBySize y CompareByCreationTime se pueden utilizar para transferir los archivos de registro. CompareByLastUpdate normalmente se utiliza para estos archivos.

FQDomain
Especifica si el agente establece un nombre de dominio y cómo:

- Si se establece en yes, el agente determinará el nombre de dominio del sistema.
- Si se establece en no, el agente no establecerá ningún nombre de dominio. Al atributo fqhostname se le asignará una serie en blanco.
- Si se establece de modo que no contenga el valor yes o no, se aceptará el nombre de dominio como valor y se añadirá al nombre de host.

Para obtener más información, consulte "Archivo de formato " en la página 671.

IncludeEIFEventAttr
El agente incluye un atributo grande denominado *EIFEvent*, que es una representación del suceso que se envía a través del EIF (Event Integration Facility) si se habilita esta característica. La información incluida en el atributo *EIFEvent* también se encuentra en otros atributos. Su tamaño grande hizo que fuera problemático, por lo tanto se ha inhabilitado de forma predeterminada. Establecer este valor en y, vuelve a habilitar el atributo EIFEvent.

Nota: La utilización de este atributo puede causar el fallo de umbrales si tiene grandes sucesos. Un suceso grande en este contexto es un suceso en el que el número total de bytes que es necesario para contener todos los valores, para todos los atributos y sus nombres, origina una serie de más de 3600 bytes.

LognameIsBasename
Cuando se establece en y, el valor del atributo Logname es el nombre base del archivo de registro en el que se ha encontrado el suceso. Esta opción sólo es aplicable a los sucesos de Performance Management. La vía de acceso se elimina. Por ejemplo, /data/logs/mylog.log se convierte en mylog.log. Si este valor se establece en n, se obtendrá la vía de acceso completa. No obstante, puesto que el atributo está limitado a 64 caracteres, si se establece en n significa que el nombre se truncará si es más largo. Por esta razón, el valor predeterminado es y. Para ver el nombre completo de la vía de acceso en un atributo más largo, puede especificarlo en la sección de correlaciones de un formato en el archivo .fmt, por ejemplo, filename FILENAME CustomSlot1. La correlación completa el atributo que se denomina filename con la vía de acceso completa del archivo en el que el suceso se ha encontrado y lo correlaciona en CustomSlot1 que tiene 256 caracteres.

LogSources
Especifica los archivos de registro de texto que se deben sondear para buscar mensajes. Se debe especificar la vía de acceso completa a cada archivo, y los nombres de archivo deben estar separados por comas. Dentro de cada nombre de archivo, también se puede utilizar un asterisco (*) para representar cualquier secuencia de caracteres, o un signo de interrogación (?), para representar cualquier carácter único. Por ejemplo, `mylog*` hace que se sondeen todos los archivos cuyos nombres empiezan por `mylog`, mientras que `mylog???` da como resultado que se sondeen todos los archivos cuyos nombres están formados por `mylog` seguidos por exactamente 3 caracteres. Estos caracteres comodín sólo se soportan dentro del nombre de archivo; la vía de acceso se debe especificar explícitamente.

Si desea utilizar expresiones regulares o coincidencia de patrón en la vía de acceso, consulte la descripción de RegexLogSources .

No es necesario que exista un origen de archivo de registro cuando se inicia el agente; el archivo de registro se sondea cuando se crea.

NewFilePollInterval
Especifica la frecuencia, en segundos, en que el agente comprueba si hay nuevos archivos para supervisar. Por ejemplo, si un nombre de archivo especificado por los valores de archivo de configuración *LogSources* o *RegexLogSources* no existe cuando se inicia el agente, éste volverá a comprobar si existen los archivos tras este intervalo.

NumEventsToCatchUp
Especifica el suceso del registro por el que empieza el agente. Esta opción proporciona cierta flexibilidad si el origen que se está supervisando es nuevo o el agente se detiene por un tiempo prolongado. Los valores siguientes son válidos:

Nota: Para los archivos de texto, son válidos los valores `0` y `-1`. Para los registros cronológicos de sucesos de Windows, son válidos los valores `0`, `-1` y n.

`0`
Empezar con el siguiente suceso en los registros. Este es el valor predeterminado.

`-1`
Cuando se establece en `-1`, el agente guarda su sitio en el archivo que se está supervisando. Guarda su sitio de modo que cuando el agente se detiene y se reinicia posteriormente, puede procesar los sucesos grabados en el registro mientras estaba detenido. De lo contrario, el agente ignorará los sucesos que hayan llegado mientras estaba detenido y se reiniciará desde el final del archivo. Este valor no es válido para conductos, ni para la supervisión de syslog en sistemas UNIX y Linux.

n
Establézcalo en un entero positivo. Empieza con el suceso número *n* desde el suceso más actual en los registros; es decir, iniciar *n* sucesos desde el suceso más actual en los registros. Si *n* es mayor que el número de sucesos que están disponibles, se procesarán todos los sucesos que estén disponibles.

Nota: El valor n sólo se puede utilizar para el registro de sucesos de Windows. El valor n se ignora cuando `UseNewEventLogAPI` se establece en *y*.

PollInterval
Especifica la frecuencia, en segundos, para sondear cada archivo de registro que se lista en la opción `LogSources` para ver si hay nuevos mensajes. El valor predeterminado es 5 segundos.

Si ha actualizado un adaptador de registro de sucesos de Windows desde un release anterior y tiene un valor establecido para `PollingInterval` en el registro de Windows, deberá especificar la opción `PollInterval` en el archivo de configuración del agente con el mismo valor que se ha utilizado en el registro de Windows. Esta regla sólo se aplica si está sustituyendo un agente de sistema operativo de Tivoli Enterprise Console que tenía valores en el registro.

ProcessPriorityClass
Especifica la prioridad del proceso para el agente. Puede ajustar este valor para mejorar el rendimiento del sistema si el agente procesa grandes volúmenes de sucesos y utiliza demasiados recursos del procesador. Los valores posibles son:

- A - Prioridad muy baja
- B - Prioridad baja
- C - Prioridad típica
- D - Por encima de la prioridad típica
- E - Prioridad alta
- F - Prioridad muy alta
- USE_CONF_FILE_VALUE - Utilice el valor especificado en el archivo de configuración. Este es el valor predeterminado.

RegexLogSources
Especifica los archivos de registro de texto que se deben sondear para buscar mensajes. Difiere de la opción LogSources en que se pueden utilizar metacaracteres de expresión regulares en la parte de nombre base del nombre de archivo y en un subdirectorio del nombre de archivo. Esta diferencia proporciona una mayor flexibilidad que la opción LogSources para describir varios archivos a supervisar en varios directorios.

Por ejemplo, especificar `/var/log/mylog*` para la sentencia LogSources es idéntico a utilizar el metacarácter punto `(.)` seguido de un metacarácter asterisco `(*)` para formar `/var/log/mylog.*` en la sentencia RegexLogSources. Este tipo de calificador hace que se sondeen todos los archivos de registro del directorio `/var/log` cuyos nombres base empiecen por `mylog` y vayan seguidos de cero o más caracteres. Un calificador `/var/log/mylog.+` origina que se sondeen todos los archivos de registro del directorio `/var/log` cuyos nombres empiecen por `mylog` y vayan seguidos de uno o más caracteres.

De modo parecido a LogSources, se debe especificar la vía de acceso completa a cada archivo y los nombres de archivo deben estar separados por comas. Sin embargo, la coma también es un carácter válido en una expresión regular. Para distinguir entre una coma que se utiliza como parte de una expresión regular y una que se utiliza para separar nombres de archivo, las comas que se utilizan como parte de una expresión regular deben tener el carácter de escape \ (barra inclinada invertida).

Por ejemplo, si desea buscar registros que coincidan con cualquiera de las siguientes expresiones regulares, `/logs/.*\.log` y `/other/logs/[a-z]{0,3}\.log`, debe utilizar el carácter de escape en la coma en la cláusula `{0,3}` de la segunda expresión para que el agente no lo confunda con el comienzo de una nueva expresión: `RegexLogSources=/logs/.*\.log,/other/logs/[a-z]{0\,3}\.log`

Si se utilizan metacaracteres en el nombre de la vía de acceso, los metacaracteres se pueden utilizar sólo en un subdirectorio de la vía de acceso. Por ejemplo, puede especificar `/var/log/[0-9\.]*/mylog.*` para tener metacaracteres en un subdirectorio. `[0-9\.]*` correlaciona cualquier subdirectorio de `/var/log` que conste exclusivamente de números y puntos `(.)`. `mylog.*` correlaciona los nombres de archivo de estos subdirectorios `/var/log` que empiezan por `mylog` seguidos por cero o más caracteres.

Dado que algunos sistemas operativos utilizan la barra inclinada invertida `(\)` como separador de directorios, ésta no se puede confundir con un metacarácter de escape de expresión regular. A causa de esta confusión, para indicar directorios se deben utilizar siempre barras inclinadas no invertidas. Por ejemplo, los archivos Windows especificados como `C:\temp\mylog.*` puede significar que `\t` es un carácter de tabulador abreviado. Por lo tanto, utilice siempre barras inclinadas `(/)` en los separadores de directorios de los sistemas operativos. Por ejemplo, `C:/temp/mylog.*` representa todos los archivos en el directorio `C:/temp` que empiezan por `mylog`.

Si hay más de un subdirectorio que contenga metacaracteres, también se emitirá un mensaje de rastreo. Por ejemplo, `c:/[0-9\.]*/temp.files/mylog.*` tiene dos subdirectorios con metacaracteres. `[0-9\.]*` es el primer subdirectorio con metacaracteres y `temp.files` es el segundo subdirectorio que utiliza un metacarácter de punto `(.)`. En este caso, el agente supone que

utiliza el primer subdirectorio con el metacarácter y se omiten los directorios subsiguientes con metacaracteres.

SubnodeName
Un valor de serie que se puede utilizar para sustituir el nombre predeterminado asignado a un subnodo de perfil de supervisión. De forma predeterminada, el nombre de subnodo asignado a un perfil de supervisión se corresponde con el nombre base del archivo de configuración utilizado para ese perfil. Con este valor se puede asignar otro nombre de subnodo.

SubnodeDescription
Un valor de serie que se puede utilizar para asignar un valor al atributo *Descripción de subnodo* de *LFAProfiles*.

UnmatchLog
Especifica un archivo para registrar sucesos descartados que no pueden ser analizados en una clase de suceso por el agente. Entonces los sucesos descartados se podrán analizar para determinar si se requieren modificaciones en el archivo de formato de agente. Los sucesos que coinciden con un patrón que utiliza *DISCARD* no aparecen en el registro de no coincidencias porque coincidían con un patrón.

Esta opción se utiliza en un entorno de prueba para validar los filtros en el archivo de formato. Esta opción llena el sistema de archivos si la deja activa durante largos períodos.

Opciones de la supervisión remota de archivos de registro mediante SSH

Aparte de **SshHostList**, que es una lista, todas las opciones pueden tener sólo un valor, que se aplica a todos los hosts que se especifican en **SshHostList**.

Sólo se da soporte a archivos de registro de texto. No se da soporte al informe de errores de AIX, syslog ni al registro de sucesos de Windows.

Consejo: Puede configurar syslog para grabar su salida en un archivo de registro de texto y luego supervisar remotamente el archivo de texto con el agente de sistema operativo.

SshAuthType
Se debe establecer en *PASSWORD* o *PUBLICKEY*. Si se establece en *PASSWORD*, el valor de **SshPassword** se trata como la contraseña que se utilizará para la autenticación SSH con todos los sistemas remotos. Si se establece en *PUBLICKEY*, el valor de **SshPassword** se trata como la contraseña que controla el acceso al archivo de claves privadas. Si se establece en *PUBLICKEY*, también se debe especificar **SshPrivKeyfile** y **SshPubKeyfile**.

SshHostList
Lista separada por comas de hosts remotos para supervisar. Todos los archivos de registro especificados en las sentencias **LogSources** o **RegexLogSources** se supervisan en cada host listado aquí. Si *localhost* es uno de los nombres de host especificados, el agente supervisa el mismo conjunto de archivos directamente en el sistema local. Cuando especifica *localhost*, no se utiliza SSH para acceder a los archivos del sistema local, sino que se leen directamente.

SshPassword
Cuando el valor de **SshAuthType** es *PASSWORD*, este valor es la contraseña de la cuenta del usuario especificado en **SshUserid**. Puede proporcionar la contraseña de la cuenta en texto sin cifrar, o puede proporcionar una contraseña que esté cifrada con el mandato **itmpwdsnmp** de la CLI de IBM Tivoli Monitoring. Para obtener más información sobre cómo cifrar una contraseña mediante el mandato **itmpwdsnmp**, consulte "Supervisión de archivo de registro remotos: cifrado de una contraseña o frase de contraseña" en la página 680.

Cuando el valor de **SshAuthType** es *PUBLICKEY*, este valor es la contraseña que descifra la clave privada especificada por el parámetro **SshPrivKeyfile**. Puede proporcionar la frase de contraseña en texto sin cifrar, o puede proporcionar una frase de contraseña que esté cifrada con el mandato **itmpwdsnmp** de IBM Tivoli Monitoring. Para obtener más información sobre cómo cifrar una contraseña mediante el mandato **itmpwdsnmp**, consulte "Supervisión de archivo de registro remotos: cifrado de una contraseña o frase de contraseña" en la página 680.

Nota: Si el valor de **SshAuthType** es *PUBLICKEY* y ha configurado que SSH no requiera una frase de contraseña, **SshPassword** se debe establecer en nulo. Para definir **SshPassword** en nulo, la entrada del archivo de configuración es:

```
SshPassword=
```

SshPort
Un puerto TCP al que conectar para SSH. Si no se establece, el valor predeterminado es *22*.

SshPrivKeyfile
Si **SshAuthType** se establece en *PUBLICKEY*, este valor debe ser la vía de acceso completa del archivo que contiene la clave privada del usuario especificado en **SshUserid** y también se debe establecer **SshPubKeyfile**. Si **SshAuthType** no se establece en *PUBLICKEY*, este valor no es necesario y se ignora.

SshPubKeyfile
Si **SshAuthType** se establece en *PUBLICKEY*, este valor debe ser la vía de acceso completa del archivo que contiene la clave pública del usuario especificado en **SshUserid** y también se debe establecer **SshPrivKeyfile**. Si **SshAuthType** no se establece en *PUBLICKEY*, este valor no es necesario y se ignora.

SshUserid
El nombre de usuario en los sistemas remotos, que el agente utiliza para la autenticación SSH.

Opción que está soportada solamente en sistemas UNIX y Linux

Linux AIX

AutoInitSyslog
Si esta opción se establece en `Yes`, el agente configurará automáticamente el recurso syslog para grabar un conjunto estándar de sucesos en un conducto que el agente supervisa. Habilitando este valor, se pueden supervisar sucesos de syslog sin tener que mantener archivos de registro continuos. Si esta opción no se establece en el archivo de configuración, es lo mismo que establecer en `No`.

Restricción: No se admite esta opción para la supervisión de archivos de registro remotos.

Opciones que están soportadas solamente en sistemas Windows

Windows

NTEventLogMaxReadBytes
Si utiliza la interfaz NT Event Log anterior (`UseNewEventLogAPI` no está establecido en y) para leer los datos del registro de sucesos en un sistema Windows, el agente leerá hasta este número de bytes cada vez que compruebe si hay nuevos datos en el registro de sucesos. Si el valor se establece en `0`, el agente intentará leer todos los nuevos datos, como hacía en releases anteriores. Esta actividad puede mantener ocupado al agente un período de tiempo considerable en un sistema con muchos sucesos. El valor predeterminado es `655360`. Cuando se establece, es posible que el agente no se detenga exactamente en el valor especificado sino en el múltiplo de un tamaño de almacenamiento intermedio interno más cercano a este valor.

PreFilter
Especifica cómo se deben filtrar los sucesos en Windows Event Log antes del proceso del agente. Las sentencias `PreFilter` se utilizan en `PreFilterMode` cuando los filtros determinan qué sucesos se envían de un registro cronológico de sucesos al agente. Un suceso coincide con una sentencia `PreFilter` cuando cada especificación *atributo=valor* de la sentencia `PreFilter` coincide con un suceso del registro de sucesos. Una sentencia PreFilter debe contener como mínimo la especificación de registro, y puede contener hasta tres especificaciones adicionales, que son opcionales: ID de suceso, tipo de suceso y origen de suceso. El orden de los atributos en la sentencia no importa.

La sentencia `PreFilter` tiene el siguiente formato básico:

```
PreFilter:Log=log_name;EventId=value; EventType=value;Source=value;
```

Puede especificar varios valores para cada atributo separando cada valor con una coma.

Cada sentencia `PreFilter` debe estar en una única línea.

`PreFilter` no es obligatorio. Todos los sucesos del registro de Windows se enviarán al agente si no se especifican prefiltros y `PreFilterMode=OUT`.

PreFilterMode
Esta opción sólo es aplicable a Windows Event Log. La opción especifica si los sucesos de registro de los sistemas Windows que coinciden con una sentencia `PreFilter` se envían (`PreFilterMode=IN`) o ignoran (`PreFilterMode=OUT`). Los valores válidos son `IN`, `in`, `OUT` o `out`. El valor predeterminado es `OUT`.

`PreFilterMode` es opcional; si no se especifica `PreFilterMode`, sólo se enviarán al agente los sucesos que no coincidan con ninguna sentencia `PreFilter`.

Nota: Si establece `PreFilterMode=IN`, también deberá definir las sentencias `PreFilter`.

SpaceReplacement
Se establece en TRUE de forma predeterminada para el registro de sucesos de Windows (solo Windows Server 2008) pero no para las versiones anteriores del registro de sucesos. Cuando `SpaceReplacement` es TRUE, los espacios del ID de seguridad, suborigen, nivel y campos de palabras clave de los mensajes del registro de sucesos se sustituyen por guiones bajos (_). Cuando `SpaceReplacement` es FALSE, los espacios en los campos de ID de seguridad, suborigen, nivel y palabras clave de los mensajes del registro de sucesos quedan sin modificar. Para más información sobre esta opción, consulte “Registro de sucesos de Windows” en la página 1054.

UseNewEventLogAPI
Cuando se establece en y en los sistemas Windows, se utiliza la nueva interfaz de Windows Event Log para los registros cronológicos de sucesos. Esta opción sólo se soporta en Windows 2008 y posteriores. Esta opción es necesaria para acceder a muchos de los nuevos registros cronológicos de sucesos presentados en Windows 2008 y las aplicaciones que se ejecutan en el mismo. Esta opción se ignora en versiones anteriores de Windows y en UNIX y Linux. Para más información sobre esta opción, consulte “Registro de sucesos de Windows” en la página 1054.

WINEVENTLOGS
Controla qué registros cronológicos de sucesos de Windows se supervisarán.

La sentencia WINEVENTLOGS es una lista delimitada por comas sin espacios. Para obtener más información, consulte “Registro de sucesos de Windows” en la página 1054.

Nota: Los retornos de carro, tabuladores o líneas nuevas de los sucesos de Windows se sustituyen por espacios.

Opción que solamente está soportada en sistemas AIX

AIX

AIXErrptCmd
Una serie de mandato **`errpt`** (informe de error) que el agente ejecuta puede proporcionarse aquí. La salida de mandato se introduce en la secuencia de datos de registro que se está supervisando.

Por ejemplo, el siguiente mandato hace que el agente busque la serie *mmddhhmmyy* y lo sustituya por la fecha y hora real de inicio. Solo se sustituye la primera aparición de la cadena.

```
AIXErrptCmd=errpt -c -smmddhhmmaa
```

Aunque puede proporcionar su propio mandato `errpt`, debe utilizar la opción `-c` (modalidad simultánea) para que el mandato se ejecute continuamente. No puede utilizar la opción `-t` ni las opciones siguientes que originan una salida detallada: `-a`, `-A` o `-g`.

La secuencia de datos es la salida estándar del mandato `errpt`, de modo que las expresiones regulares del archivo `.fmt` deben escribirse para que coincidan. Por ejemplo, la salida de datos podría ser:

```
IDENTIFIER TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
F7FA22C9   0723182911 I O SYSJ2      UNABLE TO ALLOCATE SPACE IN FILE SYSTEM
```

```
2B4F5CAB   1006152710 U U ffdc       UNDETERMINED ERROR
2B4F5CAB   1006152610 U U ffdc       UNDETERMINED ERROR
```

Un formato de ejemplo que recoge las filas de datos pero no la cabecera es:

```
REGEX GenericErrpt
^([A-F0-9]{8}) +([0-9]{10}) ([A-Z]) ([A-Z]) (\S+) +(.*)$
Identifier $1 CustomSlot1
Timestamp  $2 CustomSlot2
T          $3 CustomSlot3
C          $4 CustomSlot4
Resource   $5 CustomSlot5
msg        $6
END
```

Para obtener más información, consulte *Supervisión de un registro binario de AIX* en la publicación IBM Agent Builder: Guía del usuario.

Opciones que se aplican únicamente cuando los sucesos se reenvían a EIF

Importante: Estas opciones se aplican a sucesos EIF enviados directamente a Operations Analytics - Log Analysis, OMNIbus, o cualquier otro receptor EIF genérico. Las opciones no están pensadas para utilizarlas con el Servidor de Cloud APM.

BufferEvents
Especifica cómo se habilita el almacenamiento intermedio de sucesos. Los valores posibles son:

- **YES** - Almacena sucesos en el archivo especificado por la opción BufEvtPath (este valor es el valor predeterminado).
- **MEMORY_ONLY** - Almacena los sucesos en la memoria intermedia.
- **NO** - No almacena sucesos ni los almacena en la memoria intermedia.

BufEvtPath
Especifica el nombre completo de la vía de acceso del archivo de memoria caché del agente. Si esta vía de acceso no está corregida, el valor predeterminado es:

- AIX `/etc/Tivoli/tec/cache`
- Windows `\etc\Tivoli\tec\cache`

Nota: Si los sucesos se reenvían a más de un servidor, se debe especificar un valor *BufEvtPath* para cada canal de reenvío. Se añade un número de índice al nombre *BufEvtPath* para cada entrada adicional. Por ejemplo, utilice *BufEvtPath1* para indicar el nombre de vía de acceso del archivo de memoria caché del agente para reenviar al primer servidor adicional. El valor que se establece en cada *BufEvtPath* debe ser exclusivo.

BufEvtMaxSize
Especifica el tamaño máximo, en KB, del archivo de memoria caché del agente. El valor predeterminado es 64. El archivo de memoria caché almacena sucesos en el disco cuando la opción *BufferEvents* se establece en Yes. El tamaño mínimo del archivo es 8 KB. Los tamaños de archivo especificados por debajo de este nivel se ignorarán y se utilizará el valor de 8 KB. El valor que especifique para el tamaño máximo de archivo no tiene un límite superior.

Nota: Si el archivo de memoria caché existe, deberá suprimir el archivo para que los cambios de la opción surtan efecto.

NO_UTF8_CONVERSION
Especifica si Event Integration Facility codifica datos de sucesos en UTF-8. Cuando esta opción se establece en YES, EIF no codifica datos de sucesos en UTF-8. Se supone que los datos ya están en codificación UTF-8 cuando se pasan a EIF. Sin embargo, se añade un prefijo al distintivo para indicar que los datos están en codificación UTF-8 (si el distintivo no existe al principio de los datos de suceso). El valor predeterminado es N0.

MaxEventQueueDepth
Este valor indica el número máximo de sucesos que se pueden poner en cola para el reenvío. Cuando se alcanza el límite, cada nuevo suceso que se coloca en la cola quita el suceso más antiguo de la

cola. Si no se especifica, el valor predeterminado es 1000. Este valor es aplicable a todos los canales de reenvío si se utiliza *NumAdditionalServers*.

NumAdditionalServers
Esta entrada es necesaria si desea reenviar sucesos a más de un Netcool/OMNIbus ObjectServer. Su valor se utiliza para indicar el número de servidores a los que se reenvían sucesos. Los valores válidos son 1-8.

ServerLocation
Especifica el nombre del host en el que está instalado el servidor de sucesos. Especifique el nombre de host o la dirección IP. Utilice el formato de puntos para la dirección IP. Puede especificar valores de migración tras error como por ejemplo `ServerLocation1=2.3.4.5,2.3.4.6.` para las ubicaciones de servidor si lo desea. Si especifica valores de migración tras error para *ServerLocation*, también debe especificar un valor *ServerPort* adicional para cada *ServerLocation*.

Nota: Si los sucesos se reenvían a más de un servidor, se debe especificar un valor *ServerLocation* para cada servidor. Se añade un número de índice al nombre *ServerLocation* para cada entrada adicional. Por ejemplo, utilice *ServerLocation1* para especificar el nombre del sistema principal en el que está instalado el primer servidor adicional.

ServerPort
Especifica el número de puerto en el que el receptor EIF está a la escucha de sucesos. La opción *ServerPort* puede contener hasta ocho valores, separados por comas. Si se han especificado valores de migración tras error para *ServerLocation*, deberá establecer un valor *ServerPort* equivalente. ServerPort no se utiliza cuando se especifica la opción *TransportList*.

Nota: Si los sucesos se reenvían a más de un servidor, se debe especificar un valor *ServerPort* para cada servidor. Se añade un número de índice al nombre *ServerPort* para cada entrada adicional. Por ejemplo, utilice *ServerPort1* para especificar el número de puerto en el que el receptor EIF está a la escucha de sucesos para el primer servidor adicional.

TransportList
Especifica los nombres proporcionados por el usuario de los mecanismos de transporte, separados por comas. Cuando falla un mecanismo de transporte para las aplicaciones del remitente, la API utiliza los siguientes mecanismos de transporte en el orden especificado en la lista. Para las aplicaciones de recepción, la API crea y utiliza todos los mecanismos de transporte. Se debe especificar el tipo de transporte y el canal para cada *nombre_tipo* utilizando las palabras clave Type y Channels:

***nombre_tipo*Type**

Especifica el tipo de transporte para el mecanismo de transporte especificado por la opción *TransportList*. SOCKET es el único tipo de transporte soportado.

El servidor y el puerto para cada nombre_canal se especifican en las opciones *ServerLocation* y *ServerPort*.

***nombre_tipo*Channels**

***nombre_canal*Port**
Especifica el número de puerto en el que el servidor de mecanismos de transporte está a la escucha del canal especificado (establecido por la opción *Channel*). Cuando esta palabra clave se establece en cero, se utiliza el correlacionador de puertos. Esta palabra clave es necesaria.

***nombre_canal*PortMapper**
Habilita el correlacionador de puertos para el canal especificado.

***nombre_canal*PortMapperName**
Especifica el nombre del correlacionador de puertos si el correlacionador de puertos está habilitado.

***nombre_canal*PortMapperNumber**
Especifica el ID que está registrado por la llamada de procedimiento remoto.

***nombre_canal*PortMapperVersion**
Especifica la versión del correlacionador de puertos si el correlacionador de puertos está habilitado.

***nombre_canal*ServerLocation**
Especifica el nombre del servidor de sucesos y la región en la que está ubicado el servidor de mecanismos de transporte para el canal especificado. El canal se establece mediante la opción *Channel*. Esta palabra clave es necesaria.

El archivo de configuración acepta opciones de EIF genéricas cuando se utiliza directamente con OMNIbus. Estas opciones sólo funcionan a través de una conexión de EIF a OMNIbus. No afectan a los sucesos que se envían a Servidor de Cloud APM. Para obtener más información sobre estas opciones de EIF, consulte Palabras clave de EIF.

Archivo de formato
Los agentes del sistema operativo extraen información de los mensajes de registro del sistema y, a continuación, hacen coincidir los distintos mensajes de registro con las clases de sucesos. Para correlacionar mensajes de registro con clases de suceso se utiliza un archivo de formato como archivo de búsqueda que indica a la clase de suceso qué se debe leer, qué debe coincidir y cómo se deben formatear los datos.

Cuando el archivo de formato se utiliza como un archivo de búsqueda, todas las especificaciones de formato en el archivo se comparan desde el principio al final del archivo. Si coinciden dos clases o un mensaje tiene varias clases coincidentes, se utiliza la primera expresión que coincide desde abajo. Si no se encuentra ninguna coincidencia, se descartará el suceso. Los sucesos descartados se graban en el registro de desemparejados si se ha definido en el archivo `.conf`.

Se describe la sintaxis de expresiones regulares que se utiliza para crear patrones que coincidan con los mensajes de registro y sucesos. Se proporciona soporte de filtrado de expresiones regulares utilizando las bibliotecas ICU (International Components for Unicode) para comprobar si un valor de atributo examinado coincide con el patrón especificado.

Para más información sobre cómo utilizar expresiones regulares, consulte Expresiones regulares en la *Guía del usuario de ICU*.

Especificaciones del archivo de formato
El archivo de formato describe los patrones que el agente busca para comparar sucesos en los registros supervisados. El archivo de formato consta de una o varias especificaciones de formato.

Puede cambiar el archivo de formato mientras una instancia de agente esté en ejecución. El agente lee el archivo cuando se inicia, y se supervisa para determinar si hay cambios en su indicación de fecha y hora cada 60 segundos a partir de entonces. Si se modifica la indicación de fecha y hora del archivo, el agente reinicializa su configuración dinámicamente, sin necesidad de un reinicio. Para obtener más información, consulte “Modificación de los archivos de configuración de agente y de formato” en la página 674.

Para crear nuevos patrones para que coincidan con un suceso, utilice la sintaxis de expresiones regulares que consta de las partes siguientes:

- Cabecera de formato
- Expresión regular
- Correlaciones de atributo
- Sentencia End

La cabecera de formato contiene la palabra clave **REGEX**, que indica al agente que se está utilizando una expresión regular para coincidir con el patrón del registro supervisado.

Esta expresión regular se asigna a una clase de suceso como se muestra en el ejemplo siguiente:

```
REGEX REExample
```

Si utiliza la clase de suceso predefinida especial *DISCARD* como clase de suceso, se descartarán todos los registros que coincidan con el patrón asociado, y no se generarán sucesos para los mismos. Por ejemplo:

```
REGEX *DISCARD*
```

Cuando coincide con un patrón, no se grabará nada en el registro de desemparejados. Los registros de estado de los archivos de registro que coinciden incluyen estos sucesos descartados.

Nota: Puede asignar varias definiciones de suceso a la misma clase de suceso o a distintas clases de suceso. El nombre de clase es arbitrario y puede utilizarlo para indicar el tipo de suceso o para agrupar sucesos de distintas maneras.

Después de la cabecera de formato, el contenido del formato consta de una expresión regular en la primera línea, seguida de correlaciones. Cada correlación se muestra en una línea aparte, y estas correlaciones se describen en el ejemplo siguiente.

Todas las líneas que coinciden con las expresiones regulares se seleccionan y se envían al servidor de supervisión como sucesos. La expresión regular contiene subexpresiones. Puede utilizar las subexpresiones para comparar partes concretas de estas líneas que son iguales a una variable denominada *atributo* en EIF (Event Integration Facility).

El registro de supervisión siguiente contiene tres líneas que es posible que desee supervisar:

```
Error:  disk failure
Error: out of memory
WARNING: incorrect login
```

Por ejemplo, puede generar un suceso para un error concreto, como las líneas que empiezan por `Error` e ignorar la línea que empieza por `Warning`. La expresión regular debe coincidir con las líneas que empiecen por `Error` y también incluir una subexpresión. La subexpresión se indica mediante paréntesis y debe coincidir sólo con el texto de entrada que se quiere asignar al atributo *msg*. La siguiente definición de formato es una expresión regular simple con una sola subexpresión:

```
REGEX REExample
Error: (.*)
msg $1
END
```

En función de esta especificación de formato y el conjunto anterior de datos de registro, el agente genera dos sucesos. Ambos sucesos se asignan a la clase de suceso `REEXample`. En el primer suceso, el valor `disk failure` se asigna al atributo *msg*. También, en el segundo suceso, el valor out of memory se asigna al atributo *msg*. Puesto que la línea `Warning` no coincide con la expresión regular, se ignora y no se genera ningún suceso.

Al asignar el valor de $1 al atributo *msg*, se le asigna el valor de la primera subexpresión.

Si tiene texto del registro que contiene los siguientes errores, quizá desee asignar estos mensajes de error a su propia clase de suceso de modo que se le informe automáticamente si hay una anomalía de disco.

```
Error: disk failure on device /dev/sd0: bad sector
Error: disk failure on device /dev/sd1: temperature out of range
```

Puede incluir una descripción del disco en el que se ha producido el error y más específicamente el error de disco en el suceso.

La siguiente expresión regular contiene dos subexpresiones que identifican esta información:

```
REGEX DiskFailure
Error: disk failure on device (/dev/sd[0-9]):(.*)
device $1 CustomSlot1
msg $2
END
```

Estas dos subexpresiones se asignan a atributos de suceso. Los dos sucesos que se generan contienen los valores siguientes:

```
"device=/dev/sd0" and "msg=bad sector"
"device=/dev/sd1" and "msg=temperature out of range"
```

Si utiliza EIF para generar el primer suceso, se mostrará como se indica en el ejemplo siguiente:

```
DiskError;device='/dev/sd0';msg='bad sector';END
```

Si el suceso se envía a Servidor de Cloud APM, el atributo que se denomina *msg* se asigna al atributo del agente de Performance Management con el mismo nombre. Pero el atributo *device* no tiene ningún atributo predefinido.

Si necesita ver el valor asignado a *device* directamente en la Consola de Cloud APM, o escribir umbrales para él, debe asignarlo a un atributo de Performance Management.

El agente de sistema operativo incluye los 13 atributos predefinidos siguientes:

- Diez atributos de tipo serie que oscilan entre *CustomSlot1* y *CustomSlot10*
- Tres atributos de tipo entero que oscilan entre *CustomInteger1* y *CustomInteger3*

La utilización de estos nombres de atributo en el archivo de formato rellena los atributos de Performance Management con el mismo nombre. El uso de estos atributos no afecta al contenido del suceso EIF que se envía directamente a OMNIbus.

Nota: Los nombres de atributo `CustomSlot` y `CustomInteger` son sensibles a mayúsculas y minúsculas, por lo tanto debe especificar los nombres exactamente como se indica.

Puede asignar un atributo de la definición de suceso a uno de estos atributos de Performance Management personalizados en el archivo de formato.

Puede asignar el atributo *device* al atributo de tipo serie de Performance Management denominado *CustomSlot1* tal como se muestra en el ejemplo siguiente:

```
REGEX DiskFailure
Error: disk failure on device (/dev/sd[0-9]):(.*)
device $1 CustomSlot1
msg $2
END
```

Cuando el suceso se visualiza en Panel de instrumentos del rendimiento de aplicaciones, el valor asignado al atributo *device* se asigna al atributo `CustomSlot1` de Performance Management. Puede ver este valor en la Consola de Cloud APM o utilizarlo para definir umbrales. Puede asignar cualquier atributo en la definición de suceso a cualquiera de los 10 atributos de agente personalizados de la misma forma, utilizando "`CustomSlot`*n*", donde *n* es un número del 1 al 10, junto a la definición de atributo.

En este ejemplo, la primera subexpresión está definida específicamente como `(/dev/sd[0-9])`, pero la segunda subexpresión está definida de modo general como `(.*)`. Definiendo la expresión regular tan específicamente como sea posible, se mejora el rendimiento. Por consiguiente, si se especifica una búsqueda de un error en un dispositivo que no coincide con el mensaje de error específico que se define aquí, el procedimiento de búsqueda se detendrá inmediatamente cuando no se encuentre el error. No se pierde el tiempo buscando una coincidencia.

La palabra clave *END* completa la especificación del formato. La cabecera de formato, la expresión regular y la palabra clave *END* deben empezar cada una en una nueva línea, como se muestra en el ejemplo siguiente:

```
REGEX REExample
Error:
msg $1
END <EOL>
<EOF>
```

Nota: Para el último formato del archivo, se debe insertar una nueva línea después de la palabra clave END como se muestra en el ejemplo. De lo contrario, se producirá un error de análisis.

CustomInteger1 a *CustomInteger3* son atributos de entero personalizados de 64 bits. Puede utilizarlos del mismo modo que los atributos `CustomSlot` de tipo serie. Puede utilizar esos atributos para correlacionar atributos, subexpresiones, individuales del archivo de registro a atributos de Cloud APM individuales. Puesto que estos atributos son numéricos, puede utilizar comparaciones aritméticas, como < y >, lo que no es posible con los atributos de tipo serie.

Nota: Aunque estos valores Servidor de Cloud APM los evalúa como enteros, para fines de EIF y dentro del archivo de formato, siguen tratándose como series. Por ejemplo, para utilizar un atributo de entero en una sentencia PRINTF, deberá identificarlo con “%s”, no con “%d”.

En el ejemplo siguiente se muestra el uso de un atributo de tipo entero personalizado. Supongamos que se recibe un mensaje syslog periódico de UNIX que indica el porcentaje de un sistema de archivos que está libre, como el registro hipotético siguiente:

```
Oct 24 11:05:10 jimmy fschecker[2165]: Filesystem /usr is 97% full.
```

Puede utilizar la sentencia siguiente en el archivo de formato para comprobar el porcentaje del sistema de archivos que está libre:

```
REGEX FileSystemUsage
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2}) (.*?) (.*?):
Filesystem (.*?) is ([0-9]+)% full\.$
Month   $1 CustomSlot1
Date    $2 CustomSlot2
Time    $3 CustomSlot3
Host    $4 CustomSlot4
Service $5 CustomSlot5
Filesystem     $6 CustomSlot6
PctFull         $7  CustomInteger1
msg          PRINTF("%s: %s% full", Filesystem, PctFull)
END
```

Nota: En la sentencia anterior, todo lo que se encuentra entre los símbolos ^ y $ en la segunda y tercera línea debe estar en una única línea.

Puesto que puede haber otros sucesos que pongan valores en *CustomInteger1*, puede evitar la confusión de los distintos tipos de suceso utilizando el valor del atributo *Class* para limitar su efecto al tipo correcto de sucesos. Por ejemplo, la fórmula de umbral siguiente hace que el umbral se active sólo cuando un suceso de la clase de suceso *FileSystemUsage* tiene un valor superior o igual a 95 en *CustomInteger1*:

```
(  Class == 'FileSystemUsage' AND CustomInteger1 >= 95)
```

Un suceso diferente puede utilizar *CustomInteger1* para un propósito diferente y no desencadenará este umbral accidentalmente.

En resumen, ahora puede escribir un umbral en Performance Management que utilice operadores aritméticos en los atributos `CustomInteger`, lo cual no es posible con los atributos de `CustomSlots`.

Nota: Si correlaciona datos no enteros con los atributos `CustomInteger`, el valor resultante puede ser cero o algún valor inesperado.

Modificación de los archivos de configuración de agente y de formato

El agente del sistema operativo lee sus archivos de configuración (`.conf`) y formato (`.fmt`) cuando se inicia, y supervisa su indicación de fecha y hora cada 60 segundos.

Si se modifica la indicación de fecha y hora del archivo de configuración o formato, el agente reinicializa su configuración dinámicamente sin necesidad de un reinicio. Durante la reinicialización, la supervisión se interrumpe momentáneamente. Cuando se reanuda la supervisión, el agente debe determinar la posición en los registros supervisados desde la que se debe reiniciar. Como resultado, el agente se comporta de la misma manera que con una detención completa y un reinicio.

Nota: La reinicialización del agente después de un cambio del archivo de configuración o formato restablece la información de los grupos de atributos `Estadísticas de archivos de registro RegEx`, `Estado de archivos de registro` y `Sucesos de archivos de registro`.

De forma predeterminada, el agente inicia la supervisión a partir del final del archivo, cuando se concluye la reinicialización. Esta posición inicial puede causar que se pierdan los sucesos que se hayan producido durante la interrupción de la supervisión. Para asegurarse de que tales sucesos se recojan al reanudar la supervisión, utilice el valor `NumEventsToCatchUp=-1`.

El valor `NumEventsToCatchUp=-1` hace que se mantenga un archivo de posición. El archivo de posición se actualiza cada vez que el agente lee el archivo de registro. La actualización guarda la posición del agente en el archivo de registro, en caso de un reinicio del agente. El mantenimiento de un archivo de posición afecta levemente al rendimiento; por tanto, mantenga este archivo sólo en caso necesario. Para más información sobre `NumEventsToCatchUp`, consulte "Archivo de configuración" en la página 661.

Nota: Algunos valores de configuración no están presentes en el archivo de configuración y se establecen durante la configuración inicial. Si cambia estos valores, deberá reiniciar el agente.

Herencia

Los archivos de formato utilizan la herencia para derivar definiciones de atributo de una especificación de formato definida anteriormente.

Utilice la relación FOLLOWS para compilar especificaciones de formato específicas a partir de especificaciones de formato genéricas utilizando la herencia.

En primer lugar, defina una clase base y denomínela `DiskFailure`, por ejemplo, tal como se muestra aquí:

```
REGEX DiskFailure
Disk Failure on device (.*)
device $1 CustomSlot1
END
```

Esta expresión regular coincide con los errores `Disk Failure on device/dev/sd0` del registro de supervisión, de modo que `/dev/sd0` se asigna al atributo *device*.

No obstante, también puede ver una versión ampliada de este mensaje de error notificado en el registro de supervisión.

Por ejemplo, puede ver el mensaje de error `Disk Failure on device /dev/sd0, error code: 13`.

Este mensaje de error se correlaciona con un atributo, como se muestra en el ejemplo siguiente:

```
REGEX DiskFailureError FOLLOWS DiskFailure
Disk Failure on device (.*), error code: ([0-9]*)
errcode $2 CustomSlot2
END
```

Ahora el suceso incluye el atributo *device* y el atributo *errcode*. Dado que la clase de suceso `DiskFailure` ya ha definido un atributo para el nombre de dispositivo, se permitirá a la subclase heredar ese atributo, y esta herencia le evitará declararlo una segunda vez. El atributo se define como $1 de modo que la primera subexpresión de la expresión regular se asigna a ese atributo.

Sin embargo, la clase `DiskFailureError` también define una segunda subexpresión. Puede asignar esta subexpresión a un nuevo atributo denominado `errcode` y definirlo como $2 para hacer referencia a la segunda subexpresión de la expresión regular. Este tipo de asignación se muestra en el ejemplo anterior que muestra el texto del registro.

Ahora el suceso contiene el atributo `device` al que se asigna el valor `/dev/sd0` y el atributo `errcode` al que se asigna un valor de 13. A CustomSlot1 se le asigna el dispositivo, y a CustomSlot2 se le asigna el código de error.

Las correlaciones de atributo personalizadas de Performance Management también se heredan. Para obtener más información sobre correlaciones de atributo personalizadas de Performance Management, consulte "Especificaciones del archivo de formato" en la página 671.

Varias líneas
Utilice la sintaxis de varias líneas para emparejar registros que ocupan más de una línea con patrones del registro que está supervisando.

Especifique el carácter de nueva línea \n como parte de la expresión regular para indicar dónde se producen los saltos de línea en el registro de supervisión. Observe este tipo de sintaxis en el ejemplo siguiente:

```
REGEX REMultiLine
Line1:(.*)\nLine2(.*)
msg $1
second_msg $2
END
```

Nota: Windows Especifique una combinación de retorno de carro \r\n y nueva línea.

Si los mensajes de error siguientes se notifican en el texto del registro, se creará el suceso REMultiLine:

```
Línea1: Se ha producido un error
Línea2: El error es "error de disco"
```

Al atributo msg se le asigna el valor de `Se ha producido un error` y al atributo second_msg se le asigna el valor de `El error es "error de disco"`.

Correlaciones
El agente del sistema operativo utiliza correlaciones para determinar la clase de suceso para un mensaje de registro del sistema. El agente determina la clase de suceso emparejando el mensaje con un patrón del archivo de formato.

El agente convierte mensajes de registro en instancias de clase de suceso que contienen pares de atributo nombre=valor. Entonces, el suceso se envía al servidor de sucesos.

El agente determina la clase de suceso para un mensaje de registro del sistema en el origen. El agente determina la clase de suceso emparejando un mensaje de registro del sistema con un patrón del archivo de formato. Después de utilizar este procedimiento de coincidencias para determinar una clase, se deben asignar valores a los atributos.

Los valores de atributo provienen de distintos orígenes, como:

- Valores predeterminados proporcionados por el agente.
- Texto de registro que coincide con subexpresiones específicas de expresiones regulares

En el archivo de formato se incluye una sentencia de correlación y tiene la sintaxis siguiente:

```
nombre    valor CustomSlotn
```

Aquí se especifica cualquier identificador para describir el nombre de un atributo (también denominado variable, ranura o identificador de valor). A continuación, se debe especificar un valor para asignarlo a este atributo aplicando cualquiera de los valores descritos en “Especificadores de valor” en la página 677.

Utilice atributos personalizados para ver datos en la consola de Performance Management y para definir umbrales. Al crear umbrales, todos los valores de atributo personalizado son series. Los atributos personalizados también se requieren para que la detección de duplicados funcione porque se deben identificar los atributos que se utilizan para determinar duplicados. Para obtener más información sobre los sucesos de filtrado, consulte “Filtrado y resumen de sucesos” en la página 1052. msg es un nombre de atributo especial, con su propio atributo en la tabla de sucesos. No es necesario utilizar un atributo personalizado para msg.

Puede limitar el ámbito de un atributo de modo que sólo exista dentro de la definición de formato. Al definir el atributo, se debe preceder el nombre con un guión, por ejemplo:

```
-nombre valor
```

Los atributos que se definan de este modo no se incluirán en el suceso final. No obstante, puede hacer referencia al atributo en otra parte de la definición de formato, en concreto dentro de una sentencia PRINTF. En el ejemplo REGenericSyslog que se muestra a continuación, el atributo service no se incluye si se genera pero puede hacer referencia a él en la sentencia PRINTF. Conserva el mismo valor que se ha aplicado al atributo original cuando se ha definido sin guión. Mediante este procedimiento puede utilizar variables temporales a partir de la definición de formato que no se incluyen en el suceso final. Por ejemplo, puede definir la clase de suceso REGenericSyslog, para emparejar los sucesos syslog de UNIX del modo siguiente:

```
REGEX REGenericSyslog
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2}) (.*?) (.*?): (.*)$
month $1
date $2
time $3
host $4
-service $5
msg $6
syslog_msg PRINTF("service %s reports %s", service, msg)
END
```

Especificadores de valor
Las correlaciones de una especificación de formato asignan valores a atributos.

El componente de correlación de una especificación de formato consta de los siguientes tipos de especificadores de valor:

- $i
- Constante de tipo serie
- Sentencia PRINTF

$i

i indica la posición de una subexpresión en una serie de formato. Cada subexpresión se enumera desde 1 hasta el número máximo de subexpresiones de la serie de formato.

El valor de un especificador de valor $i (también denominado variable, ranura o atributo) es la parte del mensaje de registro del sistema que coincide con la correspondiente subexpresión.

En el ejemplo siguiente, el agente de registro convierte todos los mensajes de registro del recurso syslog de UNIX en un suceso syslog con valores asignados:

```
REGEX REGenericSyslog
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2})
 (.*?) (.*?): (.*)$
month   $1
date    $2
time    $3
host    $4
service $5
msg     $6
END
```

Cada subexpresión numerada de $1 a $6 coincide con un artículo en paréntesis en la expresión regular.

Por consiguiente, al suceso syslog siguiente:

```
Apr  6 10:03:20 jimmy syslogd 1.4.1: restart.
```

se le asignan los valores siguientes:

```
month=Apr
date=6
time=10:03:20
host=jimmy
service=syslogd 1.4.1
msg=restart.
```

Por ejemplo, en el suceso syslog, el valor `10:03:20` coincide con el tercer elemento entre paréntesis en la expresión regular, de modo que el valor se asigna al valor de tiempo *$3*. Del mismo modo, el valor `jimmy` coincide con el cuarto elemento entre paréntesis en la expresión regular, de modo que el valor se asigna al valor de host *$4*.

constante de tipo serie

La constante de tipo serie declara que el valor del atributo es la serie especificada. Si el valor de atributo es una única constante sin espacios, especifíquelo sin comillas (" ") como se muestra en el ejemplo siguiente:

```
severity WARNING
```

De lo contrario, si hay espacios en el valor de atributo, deberá utilizar comillas como se muestra en el ejemplo siguiente:

```
component "Web Server"
```

sentencia PRINTF

La sentencia PRINTF crea valores de atributo más complejos a partir de otros valores de atributo. La sentencia PRINTF consta de la palabra clave `PRINTF` seguida de una serie de formato de estilo C printf() y uno o varios nombres de atributo.

La serie de formato sólo soporta el especificador de componente `%s`. Los valores de los atributos que se utilizan en la sentencia PRINTF se deben derivar de una especificación de valor *$i* o una especificación de valor de serie de constante (no se pueden derivar de otra sentencia PRINTF).

Utilice el valor de los atributos de argumento para componer una nueva serie de constante según la serie de formato. Esta nueva serie de constante se convertirá en el valor del atributo.

Basándose en el ejemplo anterior, en el que se ha definido la clase base `REGenericSyslog` y los atributos *service* y *msg*, puede definir un atributo denominado *syslog_msg* utilizando la palabra clave `PRINTF`.

```
syslog_msg PRINTF("service %s reports %s", service, msg)
```

Si se notifica el siguiente mensaje de registro:

```
Apr  6 10:03:20 jimmy syslogd 1.4.1: restart.
```

se compondrá una nueva serie de constante que contendrá los valores de atributo de la serie de formato:

```
syslog_msg="service syslogd 1.4.1 reports restart."
```

Palabras clave
En el archivo de formato, utilice palabras clave para asignar valores que se expandan en tiempo de ejecución.

Las palabras clave siguientes se expanden en el tiempo de ejecución:

- DEFAULT
- FILENAME
- LABEL
- REGEX

DEFAULT

Utilice la palabra clave `DEFAULT` para asignar un valor DEFAULT a un determinado atributo o ranura. El agente del sistema operativo asigna un valor predeterminado interno a los atributos que se describen en la tabla siguiente:

Tabla 191. Atributos y el valor DEFAULT	
Atributos	**Descripción**
nombreHost	*nombreHost* es el nombre de host abreviado del sistema en el que se ejecuta el agente. No incluye el nombre de dominio del sistema.
origen	*origen* es la dirección IP del sistema en el que se ejecuta el agente.
nombreHostTC	*nombreHostTC* es el nombre de host totalmente calificado del sistema en el que se ejecuta el agente. Incluye el nombre de dominio del sistema.
hostRemoto	Cuando un suceso se origina en el sistema local, este atributo está vacío. Si un suceso se origina en un sistema remoto, *hostRemoto* contiene una serie con el formato *usuario@host:puerto*, que indica el nombre de host remoto en el que se produjo el suceso, y el usuario y el puerto en ese host que se utilizan para la conexión.

El valor que se asigna a *nombreHostTC* está influenciado por los siguientes valores FQDomain (opcionales) del archivo `.conf`:

- Si se establece FQDomain en `yes`, el propio agente determinará el nombre de dominio del sistema.
- Si no se establece un valor para FQDomain o si se establece el valor en `no`, el agente no establece un nombre de dominio y al atributo *fqhostname* se asigna una serie en blanco.
- Si se establece FQDomain de modo que no contenga un valor `yes` o `no`, se aceptará el nombre de dominio como valor y se añadirá al nombre de host.

En el ejemplo siguiente, la definición de formato contiene tres atributos o ranuras:

- *nombreHost* DEFAULT
- *origen* DEFAULT
- *nombreHostTC* DEFAULT

Si `FQDomain` se establece en `yes` en el archivo `.conf` y lo ejecuta en un sistema con las siguientes propiedades:

- *nombreHost*: `miHost`
- *dirección IP*: `192.168.1.100`
- *nombreDominio*: `mycompany.com`

se crea un suceso y se asignan los siguientes valores a los tres atributos:

```
"nombreHost=miHost", "origen=192.168.1.100", "nombreHostTC=miHost.mycompany.com"
```

FILENAME

La palabra clave `FILENAME` indica el nombre de archivo completo (incluida la vía de acceso) del archivo de registro que contiene el mensaje. Si utiliza un único agente para supervisar varios archivos de registro, y debe identificar el origen del suceso, utilice esta palabra clave para rellenar un atributo de suceso con el nombre de archivo. Si el mensaje proviene del registro del sistema, la correlación se establecerá en `EventLog` para los agentes del sistema operativo Windows y en `SysLogD` para los agentes del sistema operativo UNIX.

Nota: La vía de acceso incluye un atributo para esta palabra clave.

LABEL
La palabra clave LABEL especifica el nombre de host del sistema donde se ejecuta el agente.

REGEX
La palabra clave REGEX se expande a la expresión regular que coincidía con el suceso y que lo ha causado.

Longitud máxima de mensaje
Este valor es la longitud máxima de mensajes que el agente del sistema operativo puede recibir sin truncar el mensaje.

La longitud máxima de mensaje es diferente para Performance Management y Tivoli Netcool/OMNIbus.

Performance Management
Para los sucesos enviados a Performance Management, el atributo `msg` está limitado a 2048 bytes. Los mensajes con una longitud superior se truncarán.

Tivoli Netcool/OMNIbus
Para los sucesos enviados a través de Probe for Tivoli EIF a Netcool/OMNIbus, el tamaño total del suceso, incluido el nombre de clase y todos los atributos y sus valores no puede superar los 4096 bytes. Por ejemplo, en el siguiente suceso EIF de muestra, `;END` no se tiene en cuenta en el límite de 4096 bytes. Sin embargo, todo lo demás sí que cuenta para el límite, incluidos los elementos de sintaxis como, por ejemplo, los puntos y coma, las comillas y los signos de igual.

```
Class;attr1=value1;attr2=value2;msg='Hello, world';END
```

Supervisión de archivo de registro remotos: cifrado de una contraseña o frase de contraseña

Para aumentar la seguridad, puede cifrar las contraseñas y las frases de contraseña que se transmiten a sistemas remotos cuando se utiliza Supervisión de archivos de registro remotos.

Acerca de esta tarea

Las frases de contraseña y contraseñas cifradas se almacenan en el archivo de configuración (`.conf`). Para obtener más información sobre el archivo de configuración, consulte "Archivo de configuración" en la página 661.

Procedimiento

- Ejecute el mandato **`itmpwdsnmp`** y proporcione la contraseña o frase de contraseña que se va a cifrar:
  - Linux AIX El mandato se ejecuta desde el directorio de instalación de Cloud APM. La vía de acceso de instalación predeterminada es `opt/ibm/apm/agent` y *dir_instalación* es donde ha instalado el agente.
  - Windows La vía de acceso de instalación predeterminada es `C:\IBM\APM`.

  Linux Ejemplo del mandato cuando se ejecuta en un sistema Linux:

```
$ export dir_instal=/opt/ibm/apm/agent/bin
$ /opt/ibm/apm/agent/bin

Especifique la serie que se desea cifrar:
micontraseña

Confirme la serie:
micontraseña

{AES256:keyfile:a}Z7BS23aupYqwlXb1Gh+weg==
$
```

  En el ejemplo, toda la salida del mandato `{AES256:keyfile:a}Z7BS23aupYqwlXb1Gh+weg==` se utiliza para establecer **`SshPassword`** en el archivo de configuración del agente. El prefijo `{AES256:keyfile:a}` indica al agente que la contraseña está cifrada.

  Para cifrar una frase de contraseña para un archivo de claves privadas, siga el mismo procedimiento.

Configuración de scripts personalizados del agente de sistema operativo

Los agentes de Monitoring Agent for Linux OS, Monitoring Agent for UNIX OS y Monitoring Agent for Windows OS se configuran automáticamente. Esta característica permite a los usuarios definir scripts para que se ejecuten en los agentes de sistema operativo con una frecuencia definida.

La característica de scripts personalizados está habilitada de forma predeterminada. El administrador puede habilitarla/inhabilitarla estableciendo una nueva variable de entorno *KXX_FCP_SCRIPT*=true/false (el valor predeterminado es true) en el archivo de configuración de agente, donde XX puede ser:

- LZ para Monitoring Agent for Linux OS

- UX para Monitoring Agent for UNIX OS

- NT para Monitoring Agent for Windows OS

Los detalles se proporcionan en las secciones siguientes.

Inicio rápido de script personalizado

Añada un script personalizado para los agentes de sistema operativo para definir scripts para que se ejecute en agentes de sistema operativo con una frecuencia definida.

La característica se habilita con los valores predeterminados tan pronto como se inicia el agente de sistema operativo. La única acción para iniciar la característica de script es:

Crear un archivo de propiedades bajo el directorio predeterminado (en Linux™ o UNIX™ es `dir_instalación/localconfig/`*`código_producto`*`/scripts_definitions`, en Windows™ es `dir_instalación\localconfig\nt\scripts_definitions`) utilizando como ejemplo la plantilla proporcionada `script_property.txt`.

Sólo son necesarias dos propiedades:

ATTRIBUTE_NAME
Cualquier nombre utilizado para identificar de forma exclusiva la definición de script en el archivo de propiedades.

SCRIPT_PATH_WITH_PARMS
La vía de acceso completa del script con argumentos.

Se pueden utilizar no sólo scripts de shell sino también perl y otros tipos de scripts. Especifique el mandato completo para ejecutarlo en la propiedad SCRIPT_PATH_WITH_PARMS.

Por ejemplo, `perl C:\IBM\scripts\Custom_Scripts\date.pl`. En este ejemplo, asegúrese de que la ubicación de `perl` la puede resolver el agente mediante la variable PATH del entorno. De lo contrario, especifique la vía de acceso completa donde está instalado `perl`.

Parámetros de archivos de entorno de agente de sistema operativo

Puede establecer los parámetros para los scripts personalizados en los archivos de entorno del agente del sistema operativo.

Es posible personalizar la función de scripts estableciendo parámetros en los archivos de entorno del agente del sistema operativo:

***dir_instalación*/config/lz.environment**
El archivo de entorno para Monitoring Agent for Linux OS.

***dir_instalación*/config/ux.environment**
El archivo de entorno para Monitoring Agent for UNIX OS.

***dir_instalación*\TMAITM6_x64\KNTENV**
El archivo de entorno para Monitoring Agent for Windows OS de 64 bits.

***dir_instalación*\TMAITM6\KNTENV**
El archivo de entorno para Monitoring Agent for Windows OS de 32 bits.

KXX_FCP_SCRIPT
La función de scripts está habilitada de forma predeterminada. Para inhabilitarla, establezca: `KXX_FCP_SCRIPT=false`

Pueden definirse otros parámetros dentro de los archivos de entorno del agente en función de necesidades específicas:

KXX_FCP_SCRIPT_DEFINITIONS

La ubicación donde se almacenan los archivos de propiedades.

La ubicación predeterminada en Linux™ o UNIX™ es *dir_instalación*/localconfig/*PC*/scripts_definitions; en Windows™, es *dir_instalación*\localconfig \nt \scripts_definitions

KXX_FCP_SCRIPT_INTERVAL

El agente del sistema operativo utiliza el valor de esta variable como intervalo de bucle en segundos para comprobar la ejecución de los scripts en ejecución y envía sucesos si se satisface la condición de filtro. El valor mínimo es de 30 segundos y el valor máximo es de 300 segundos. Los valores no válidos se restablecen en el valor predeterminado. El valor predeterminado es 60 segundos.

Nota: Este parámetro se ignora si KXX_FCP_SCRIPT_SYNC_INTERVALS se establece en USE_SCRIPT (consulte la definición de KXX_FCP_SCRIPT_SYNC_INTERVALS).

KXX_FCP_SCRIPT_SYNC_INTERVALS

Si el intervalo de bucle del agente definido por KXX_FCP_SCRIPT_INTERVAL es mayor que la frecuencia de ejecución de script, puede ocurrir que los datos generados por algunos de los bucles de ejecución de script se pierdan. A fin de evitar este comportamiento, la frecuencia de ejecución de script se puede sincronizar con el intervalo de bucle de agente estableciendo KXX_FCP_SCRIPT_SYNC_INTERVALS en:

- USE_AGENT - El valor de frecuencia de ejecución de cada script se fuerza al valor máximo entre KXX_FCP_SCRIPT_INTERVAL y la EXECUTION_FREQUENCY definida en su archivo de propiedades.
- USE_SCRIPT - El intervalo de bucle de agente se establece dinámicamente en el valor de frecuencia mínima (EXECUTION_FREQUENCY en el archivo de propiedades) entre todos los scripts definidos. El valor establecido por KXX_FCP_SCRIPT_INTERVAL se ignora. La frecuencia de los scripts permanece tal como se define en los archivos de propiedades. Si se establece USE_SCRIPT, el intervalo de bucle de agente puede cambiar cada vez que se añade, cambia o elimina una definición de script. En cualquier caso, no puede ser menor que el valor establecido por KXX_FCP_OVERRIDE_MIN_FREQUENCY_LIMIT ni superior a 300 segundos.
- NO - No se realiza ninguna sincronización y es posible que algunos resultados de ejecución se pierdan.

KXX_FCP_SCRIPT_DEFINITIONS_CHECK_INTERVAL

Durante el inicio y en cada intervalo definido por esta variable, el agente de sistema operativo comprueba si hay cambios en los scripts o en los archivos de propiedades. Tenga en cuenta que si KXX_FCP_SCRIPT_DEFINITIONS_CHECK_INTERVAL es menor que el intervalo de bucle de agente, se restablece en el intervalo de bucle de agente. El valor máximo permitido es el valor predeterminado, 300 segundos.

KXX_FCP_USER

Este parámetro sólo es válido en los agentes de sistema operativo Linux™ o UNIX™. Define el usuario utilizado para crear el proceso fcp_deamon si es distinto del usuario de proceso del agente de sistema operativo; este usuario ejecuta todos los scripts. Tenga en cuenta que el propietario del agente de sistema operativo debe tener el permiso adecuado para crear el proceso fcp_daemon. En Windows™, debe definirse un usuario distinto como inicio de sesión del servicio de Monitoring Agent for Windows OS "FCProvider". El usuario debe tener permiso de "Control completo" sobre el directorio de instalación del agente y los directorios de repositorio de scripts. Para obtener más información, consulte:

https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/install_linuxaix_agent_nonroot.html

KXX_FCP_MAX_CDP_DP_THREAD_POOL_SIZE
Define el número máximo de script simultáneos que deben ejecutarse. El valor máximo es 32.

KXX_FCP_MAX_DAEMON_RESTARTS

El agente de sistema operativo observa el proceso fcp_daemon: si se produce una salida anómala del proceso, el agente del sistema operativo lo reinicia. El valor predeterminado es 4. El reinicio se realiza según el valor de KXX_FCP_MAX_DAEMON_RESTARTS (veces al día). Debe utilizarse el valor 0 para evitar el reinicio; si se establece -1, el agente de sistema operativo reintenta reiniciar fcp_daemon indefinidamente. El contador de reinicios se restablece durante el reinicio del agente del sistema operativo.

KXX_FCP_SEND_SCRIPT_RUNTIME_EVENTS
El valor predeterminado es true. Si se establece en false, el agente de sistema operativo detiene el envío de sucesos para cada fila de salida estándar de script. En este caso, las salidas de script son visibles en los espacios de trabajo de la consola, pero no se visualizan situaciones y no se recopilan datos históricos.

KXX_FCP_OVERRIDE_MIN_FREQUENCY_LIMIT

Se utiliza cuando KXX_FCP_SCRIPT_SYNC_INTERVALS se establece en USE_SCRIPT. En esta condición, establece el valor mínimo del intervalo de bucle de agente de sistema operativo.

El uso de valores bajos para el intervalo de bucle de agente de sistema operativo (inferior a 5 segundos) es muy invasivo y puede afectar al rendimiento de los agentes del sistema operativo. Si es necesaria una recopilación de datos frecuente (por ejemplo, cada segundo), se sugiere personalizar un script. El script almacena en memoria caché los datos con la frecuencia necesaria y devuelve los datos recopilados al agente de sistema operativo con un intervalo mayor (por ejemplo, cada 60 segundos).

También pueden utilizarse las siguientes variables (CDP) de Agent Builder para controlar el comportamiento del proceso fcp_daemon:

CDP_DP_REFRESH_INTERVAL
(valor predeterminado 60 seg) Hora de inicio planificada de script global. Se utiliza si no se pasa la frecuencia en el archivo de propiedades de script.

CDP_DP_SCRIPT_TIMEOUT
(valor predeterminado 30 seg) Tiempo máximo de ejecución de script global. Cuando el tiempo de ejecución de un script supera este límite, su código de estado (Status_Code) se establece en TIMEOUT

CDP_DP_KILL_ORPHAN_SCRIPTS
(Y|N - valor predeterminado N) Comportamiento global utilizado por el proceso fcp_daemon para los scripts que agotan el tiempo de espera. Si se establece en 'Y ', los scripts finalizan; de lo contrario, se abandonan. Este valor se ignora para un script específico si se establece la clave KILL_AFTER_TIMEOUT en el archivo de propiedades de script.

CDP_MAXIMUM_ROW_COUNT_FOR_CPCI_DATA_RESPONSES
(valor predeterminado 1000) El valor global se añade por razones de rendimiento para limitar el número máximo de filas de salida devueltas por los scripts. Las filas adicionales una vez alcanzado este límite se ignoran. Los valores permitidos son enteros positivos. Los valores no válidos se modifican a sin límite.

El proceso fcp_daemon también admite las otras variables de entorno que se utilizan para controlar los agentes de Agent Builder. Para obtener una lista completa, consulte la documentación oficial de Agent Builder aquí:

http://www-01.ibm.com/support/knowledgecenter/api/redirect/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/agentbuilder63_user.pdf

Parámetros de los archivos de propiedades
Puede establecer los parámetros para los scripts personalizados en los archivos de propiedades.

El directorio KXX_FCP_SCRIPT_DEFINITIONS contiene una lista de archivos *.properties. Cada archivo de propiedades contiene una lista de scripts que se deben ejecutar con las respectivas propiedades en el

formato de `clave=valor`. Las propiedades que se pueden definir (no sensibles a mayúsculas y minúsculas) son:

ATTRIBUTE_NAME

Necesaria: serie de 256 caracteres como máximo. Un nombre de su elección que defina un script específico y sus atributos. Los caracteres que se pueden utilizar para el nombre `ATTRIBUTE NAME` pueden ser alfanuméricos y sólo se puede utilizar el subrayado como carácter especial. Si se utilizan otros caracteres especiales (espacio o blanco), se convierten a subrayado (_). Cuando se listan varios scripts en el mismo archivo de propiedades, se deben especificar más `ATTRIBUTE_NAME` diferentes (uno para cada script). Debe ser el primer valor que se especifica para cada script definido y delimita el inicio de las propiedades establecidas para el script específico hasta el siguiente `ATTRIBUTE_NAME`.

SCRIPT_PATH_WITH_PARMS

Necesaria: serie de 512 caracteres como máximo. Este parámetro define la vía de acceso completa al script con parámetros, que están separados por un espacio en blanco. No se pueden utilizar caracteres especiales en el nombre de vía de acceso de script. Los valores que contienen blancos deben especificarse entre comillas simples (') o comillas dobles ("). Se pueden pasar variables de entorno, pero sólo entre ${...} para todos los sistemas operativos. Las variables de entorno deben estar disponibles en el contexto de proceso de agente de sistema operativo.

EXECUTION_FREQUENCY

Opcional: el valor predeterminado es 60 segundos. Este parámetro define la frecuencia de ejecución de script.

CUSTOM_NAME

Opcional: serie de 256 caracteres como máximo. Este parámetro se puede utilizar para especificar una descripción del script.

IS_ACTIVE

Opcional: true|false. El valor predeterminado es true. Activa el script. Si es false, el script no se ejecuta.

DISABLE_USE_AGENT_SYNC

Opcional: true|false. El valor predeterminado es false. Si el valor es true, también se respeta `EXECUTION_FREQUENCY` del script si la variable global `KXX_FCP_SCRIPT_SYNC_INTERVALS` está establecida en `USE_AGENT`.

KILL_AFTER_TIMEOUT

Opcional: true|false. El valor predeterminado lo define la variable `CDP_DP_KILL_ORPHAN_SCRIPTS`. Si es true, el script finaliza después del tiempo de espera. Se produce un tiempo de espera cuando la ejecución de script es mayor que el valor especificado por el parámetro `CDP_DP_SCRIPT_TIMEOUT` en el archivo de configuración de agente de sistema operativo. En caso contrario, se ignora. En ambos casos, no se recopilan datos. Tenga en cuenta que cuando se establece `KILL_AFTER_TIMEOUT`, sólo finaliza el script definido en el archivo de propiedades, y no los procesos hijo (si existen) creados por el script. Esta característica no recibe soporte de los agentes de sistema operativo Solaris™ y Windows™ de 32 bits y los scripts que superan el tiempo de espera se abandonan.

as filas de salida devueltas por un script se analizan.

El script devuelve una salida estándar (a la que se llama como primera señal). Cuando el script devuelve más valores en la fila de salida, estos se añaden como más señales. Un máximo de cinco series, cinco enteros y cinco flotantes siguiendo una sintaxis predefinida.

OUTPUT_TYPE

STRING|INTEGER|FLOAT - Opcional: El valor predeterminado es string. Define el tipo de la primera señal devuelta por cada fila del script; OUTPUT_TYPE puede ser:

- STRING (valor predeterminado): series de hasta 2048 caracteres. Cuando se utiliza, la primera señal completa el atributo "Standard_Output_String" de `KXX_Custom_Scripts_Rtm_Smp`.
- INTEGER: permite obtener valores numéricos entre -9223372036854775806 y 9223372036854775806. Cuando se utiliza, la primera señal completa el atributo "Standard_Output_Integer" de `KXX_Custom_Scripts_Rtm_Smp`.

- FLOAT: permite obtener valores numéricos entre -92233720368547758.06 y 92233720368547758.06, con dos precisiones decimales. Cuando se utiliza, la primera señal completa el atributo "Standard_Output_Float" de KXX_Custom_Scripts_Rtm_Smp.

TOKEN_TYPES
STRING|INTEGER|FLOAT: Opcional. Define el tipo de salida de más señales después de la primera. El usuario puede definir un máximo de cinco series, cinco enteros y 5 flotantes. Es una lista de tipos separados por comas: <tipo_señal>,<tipo_señal>,... tipo_señal puede estar vacío o ser uno de los siguientes (no sensible a mayúsculas y minúsculas):

- - STRING o S
- - INTEGER o I
- - FLOAT o F
- Si *TOKEN_TYPES* está vacío, se salta la señal correspondiente.

  Ejemplos de los mismos diseños válidos:
- - TOKEN_TYPES=S,I,S,,,F,,F,F
- - TOKEN_TYPES=String,integer,S,,,Float,,f,FLOAT

TOKEN_LABELS
STRING: Opcional. Máximo de 16 caracteres cada etiqueta. Define las etiquetas de las señales que se definen en TOKEN_TYPES. Este valor es una lista de etiquetas de señal separadas por comas y deben corresponder a las señales definidas por TOKEN_TYPES. Por ejemplo:

- TOKEN_TYPES=S,I,S,,,F,,F,F
- TOKEN_LABELS=Nombre Cpu,Número Cpu,Descripción,,,valor 1,,valor 2,valor 3
- TOKEN_LABELS se ignora si no se ha establecido TOKEN_TYPES.

TOKEN_SEPARATOR
Opcional: punto y coma ";" predeterminado. Establece la cadena que se debe utilizar como separador para dividir la fila de salida en señales. It se ignora si no se ha establecido TOKEN_TYPES. Se acepta un valor vacío (blanco) como separador y varios blancos consecutivos en las filas de salida se consideran como uno solo.

Los dos parámetros siguientes permiten filtrar la salida de filas de un script. El agente de sistema operativo los aplica sólo en la primera señal y se deben utilizar juntos:

FILTER_VALUE
Opcional. El valor utilizado para la comparación. Es necesario si se ha definido FILTER_OPERADOR. Si OUTPUT_TYPE es una serie, el valor de filtro debe reflejar exactamente el valor de serie devuelto por el script que está destinado a filtrarse, sin comillas adicionales (no se permiten comodines).

FILTER_OPERATOR
Opcional. El operador utilizado para la comparación. Es necesario si se ha definido FILTER_VALUE. Los valores de FILTER_OPERATOR aceptados incluyen:

- = (igual a)
- != (no igual a)
- > (mayor que) sólo para tipo numérico
- >= (no inferior a) sólo para tipo numérico
- < (menor que) sólo para tipo numérico
- <= (no mayor que) sólo para tipo numérico

Ejemplos de archivo de propiedades
Ejemplos de valores de parámetros en los archivos de propiedades.

#Definición de primer script: el script ex_script1.sh se inicia cada 150 segundos. Devuelve valores flotantes y el agente sólo tiene en cuenta las filas de salida iguales a 0.5.

```
ATTRIBUTE_NAME=sample1
SCRIPT_PATH_WITH_PARMS=/opt/ibm/apm/agent/localconfig/lz/scripts_definitions/ex_script1.sh
EXECUTION_FREQUENCY=150
OUTPUT_TYPE=FLOAT
FILTER_VALUE=0.5
FILTER_OPERATOR==
```

#Definición de segundo script: el script ex_script2.sh se inicia cada 60 segundos. Devuelve valores enteros y el agente sólo tiene en cuenta las filas diferentes de 0.

```
ATTRIBUTE_NAME=ex_script2
SCRIPT_PATH_WITH_PARMS=${CANDLE_HOME}/tmp/check_out.sh
EXECUTION_FREQUENCY=60
OUTPUT_TYPE=INTEGER
FILTER_VALUE=0
FILTER_OPERATOR=!=
```

#Definición de tercer script: el script ex_script3.sh se inicia cada 120 segundos con tres parámetros de entrada (el primer parámetro de entrada es un entero, el segundo y el tercero son series). Finaliza si se cuelga o si el tiempo de ejecución es mayor que el valor de tiempo de espera.

```
ATTRIBUTE_NAME=ex_script3
SCRIPT_PATH_WITH_PARMS=/opt/scripts/ex_script3.sh 1 "segundo parámetro de entrada" "tercer
parámetro de entrada"
EXECUTION_FREQUENCY=120
OUTPUT_TYPE=STRING
KILL_AFTER_TIMEOUT=TRUE
```

#Definición de cuarto script: el script cpu_mem_percentage.sh se inicia cada 50 segundos y devuelve el cpuid como serie de salida estándar y dos valores flotantes para el porcentaje de CPU desocupada y utilizada y dos enteros para el uso de memoria y de memoria virtual. Se utiliza la barra vertical como separador para analizar la salida. A continuación figura un ejemplo de fila que el script debe devolver:

cpu2|35,5|65,5|3443|123800

```
ATTRIBUTE_NAME=cpu and mem Usage
SCRIPT_PATH_WITH_PARMS=${SCRIPT_HOME}/cpu_mem_percentage.sh
OUTPUT_TYPE=STRING
TOKEN_TYPES=F,F,I,I
TOKEN_LABELS= Idle CPU %, Used CPU %, Virt MEM used MB, MEM used MB
TOKEN_SEPARATOR=|
EXECUTION_FREQUENCY=50
```

Problemas y limitaciones conocidos

Problemas y limitaciones conocidos

- La característica de script no se soporta en sistemas Windows™ 2003 de 64 bits.
- La operación kill (terminar) después de un tiempo de espera no funciona en los agentes de los sistemas operativos Solaris™ y Windows™ de 32 bits.
- El fcp_daemon puede detener la ejecución de scripts en Windows™ de 32 bits si algunos scripts no se completan dentro del periodo de tiempo de espera y el usuario ha habilitado el rastreo intensivo. Si fcp_daemon deja de ejecutar scripts, los datos indicados en la consola reflejan la última hora que se ha ejecutado el script. También es posible que el agente de sistema operativo deje de devolver datos. La detención del proceso fcp_daemon permite que el agente reanude la operación apropiada.
- Se devuelve SCRIPT_NONZERO_RETURN en lugar de SCRIPT_NOT_FOUND o SCRIPT_LAUNCH_ERROR en Solaris™.
- La característica de script no proporciona la globalización completa; pueden surgir algunos problemas al utilizar caracteres nacionalizados en archivos de propiedades o resultados de script.
- En el agente de sistema operativo Windows™, no hay ninguna posibilidad de ejecutar scripts que residen en una unidad de red correlacionada.
- Cuando se actualiza el agente de sistema operativo Windows™, la característica de script no está habilitada de forma predeterminada. Edite KNTENV y cambie `KNT_FCP_SCRIPT=FALSE` por `KNT_FCP_SCRIPT=TRUE`.

Resolución de problemas de scripts personalizados
Resolución de problemas de scripts personalizados

La variable *KBB_RAS1* estándar se aplica al agente del sistema operativo y a los procesos fcp_daemon. Para aplicar un valor de rastreo específico sólo a fcp_daemon, utilice la variable *KXX_FCP_KBB_RAS1*; si se establece *KXX_FCP_KBB_RAS1*, fcp_daemon ignorará el valor especificado por *KBB_RAS1*.

Para rastrear las operaciones registradas por las hebras principales del agente de sistema operativo de la característica:

```
KBB_RAS1=ERROR (UNIT:factory ALL)
```

Para rastrear las consultas de scripts desde el servidor APM y los sucesos enviados al servidor, añada las entradas:

En el Monitoring Agent for Linux OS

```
(UNIT:klz34 ALL) (UNIT:klz36 ALL)
```

En el Monitoring Agent for UNIX OS

```
(UNIT:kux48 ALL) (UNIT:kux50 ALL)
```

En el Monitoring Agent for Windows OS

```
(UNIT:knt84 ALL) (UNIT:knt86 ALL)
```

Para ver los rastreos de TEMA para verificar la ejecución de situaciones privadas, añada las entradas:

```
(UNIT:kraavp all) (UNIT:kraapv all)
```

Para ver la ejecución de los scripts y cómo se analizan los datos de los scripts, establezca:

```
KXX_FCP_KBB_RAS1=Error (UNIT:command ALL)
```

Para resolver los problemas de comunicación entre el agente de sistema operativo y fcp_daemon, añada este nivel de rastreo a *KBB_RAS1* y a *KXX_FCP_KBB_RAS1*:

```
(UNIT:cps_socket FLOW) (UNIT:cpci FLOW)
```

Para ver la interacción entre el proceso del agente de sistema operativo y fcp_daemon con detalle, añada a *KBB_RAS1* y *KXX_FCP_KBB_RAS1*:

```
(UNIT:cps_socket ALL) (UNIT:cpci ALL)
```

Escenario de inicio rápido
En esta sección se describen los pasos mínimos necesarios para configurar los scripts personalizados para un escenario de ejemplo.

La sección siguiente describe los pasos mínimos que es necesario realizar para configurar un Monitoring Agent for Linux OS para ejecutar dos scripts personalizados.

Descripciones de scripts personalizados

En este ejemplo, el usuario tiene dos scripts bajo un directorio /scripts_repo:

checkDIRsize.sh: este script comprueba el tamaño de un directorio especificado que se pasa como parámetro de entrada. La salida es un entero como: `4594740`

cpu_mem_usage.sh: este script comprueba los porcentajes de CPU utilizados y los megabytes de memoria de intercambio utilizados. La salida se devuelve con el formato: `cpu1|96 ,5|23800`

Donde la primera señal es el ID de CPU, la segunda señal es el porcentaje de CPU utilizado, la tercera señal es la memoria de intercambio utilizada en megabytes.

La personalización necesaria para que Monitoring Agent for Linux OS ejecute estos scripts.

La característica se habilita con los valores predeterminados tan pronto como se inicia el agente de sistema operativo:

Cree archivos de propiedades AnyName.`properties` bajo el directorio predeterminado `dir_instalación/localconfig/lz/scripts_definitions`. En este ejemplo, cree dos archivos de propiedades, uno para cada script, denominados checkDIRsize.properties y cpu_mem_usage.properties:

```
#CheckDIRsize.properties
ATTRIBUTE_NAME=OPT_DIR_SIZE
SCRIPT_PATH_WITH_PARMS=/scripts_repo/checkDIRsize.sh /opt
EXECUTION_FREQUENCY=20
OUTPUT_TYPE=INTEGER
```

```
#cpu_mem_usage.properties
ATTRIBUTE_NAME=cpu_mem_usage
SCRIPT_PATH_WITH_PARMS=/scripts_repo/cpu_mem_percentage.sh
OUTPUT_TYPE=string
TOKEN_TYPES=F,I
TOKEN_LABELS= Used CPU %, Swap MEM used MB
TOKEN_SEPARATOR=|
EXECUTION_FREQUENCY=10
```

No es necesario reiniciar el agente de sistema operativo después de añadir (o cambiar) los dos archivos de propiedades. El agente de sistema operativo comprueba el directorio de definición de script con un intervalo de tiempo especificado (el valor predeterminado es de 300 segundos). Abra la consola y, bajo el espacio de trabajo "Scripts personalizados", se muestran los detalles y resultados de los scripts.

Configuración de la recopilación de datos del sistema de archivos del sistema operativo Linux

Monitoring Agent for Linux OS se configura automáticamente. Sin embargo, puede configurar el comportamiento de la recopilación de datos del sistema de archivos.

Monitoring Agent for Linux OS tiene un comportamiento predeterminado para la recopilación de datos del sistema de archivos.

El comportamiento predeterminado consiste en supervisar sólo los sistemas de archivos de `/etc/fstab`. Se define una variable de entorno *KBB_SHOW_MTAB_FS* en el archivo `lz.environment` para controlar el comportamiento de la recopilación de datos del sistema de archivos. Si desea supervisar todos los sistemas de archivos (listados en `/etc/fstab` y `/etc/mtab`), puede establecer KBB_SHOW_MTAB_FS=true.

KBB_SHOW_MTAB_FS
Esta variable está disponible en el archivo *`dir_instalación`*`/config/.lz.environment`. El valor predeterminado es `false` y define que el agente debe supervisar sólo los sistemas de archivos de `/etc/fstab`. Si desea supervisar todos los sistemas de archivos (listados en `/etc/fstab` y`/etc/mtab`), cambie el valor a `true`. Por ejemplo, *KBB_SHOW_MTAB_FS=true*.

Configuración de la supervisión de PHP

Debe configurar el Monitoring Agent for PHP para que el agente pueda recopilar datos de la aplicación PHP que se está supervisando.

Antes de empezar

1. Asegúrese de instalar el paquete php-process. Si utiliza el mandato `yum install` para instalar PHP, ejecute el mandato `yum install php-process` para instalar el paquete php-process.
2. Asegúrese de que el servidor Apache HTTPD esté iniciado antes de configurar el agente.

Abra el archivo de configuración `httpd.conf` del servidor HTTP Apache y asegúrese de que las opciones `mod_status` y `ExtendedStatus On` estén habilitadas. Por ejemplo:

```
ExtendedStatus On
<Location /server-status>
        SetHandler server-status
        Order deny,allow
        Allow from all
        Allow from 127.0.0.1
</Location>
```

En el ejemplo dado, `http://127.0.0.1/server-status` debe funcionar bien para que el agente funcione adecuadamente.

Nota: Debe tener Lynx o Links instalado en Linux para que el agente obtenga datos de supervisión.

Asegúrese de que el mandato `apachectl status` funciona bien en el servidor Apache supervisado sin cambios de código para el mandato `apachectl`. Lynx debe estar instalado para que el mandato `apachectl status` funcione adecuadamente.

Acerca de esta tarea

Para evitar problemas de permisos al configurar el agente, asegúrese de utilizar el mismo ID de usuario root o no root que se utilizó para instalarlo. Si ha instalado el agente mediante un usuario seleccionado y desea configurar el agente mediante un usuario distinto, consulte "Configuración de agentes como usuarios no root" en la página 191. Si ha instalado y configurado el agente mediante un usuario seleccionado y desea iniciar el agente mediante un usuario distinto, consulte "Inicio de agentes mediante un usuario no root" en la página 1047.

El Agente de PHP es un agente de varias instancias; debe crear la primera instancia e iniciar el agente de forma manual. El Nombre de sistema gestionado incluye el nombre de instancia que especifique, por ejemplo, *instance_name*`:`*nombre_host*`:`*pc*, donde *pc* es el código de producto de dos caracteres. El Nombre de sistema gestionado está limitado a 32 caracteres. El nombre de instancia que especifique está limitado a 28 caracteres menos la longitud del nombre de host. Por ejemplo, si especifica PHP2 como nombre de instancia, el nombre de sistema gestionado será `PHP2:nombrehost:PJ`.

Importante: Si especifica un nombre de instancia largo, el Nombre de sistema gestionado queda truncado y el código de agente no se visualiza correctamente.

Procedimiento

- Si su entorno es el mismo que los valores predeterminados, puede utilizar la vía de acceso binaria de ejecución, el archivo `php.ini` predeterminado y el puerto predeterminado para configurar el agente:
  a) Escriba:
  dir_instalación`/bin/php-agent.sh config` *nombre_instancia dir_instalación*`/samples/php_silent_config.txt`
  Donde *nombre_instancia* es el nombre que desea dar a la instancia y *dir_instalación* es el directorio de instalación de Agente de PHP. El directorio de instalación predeterminado es `/opt/ibm/apm/agent`.
  b) Para iniciar el agente, especifique:
  dir_instalación`/bin/php-agent.sh start` *nombre_instancia*
- Para configurar el agente mediante la edición del archivo de respuestas silencioso y la ejecución del script sin interacción, siga estos pasos:
  a) Abra *dir_instalación*`/samples/php_silent_config.txt` en un editor de texto.
  b) En **Ubicación del binario de ejecución de PHP**, puede especificar el directorio en el que está ubicada la ejecución de PHP. La ubicación predeterminada es `/usr/local/bin`.
  c) En **Ubicación del archivo INI de PHP** puede especificar el directorio donde se encuentre el archivo `php.ini`. La ubicación predeterminada es `/etc`.
  d) En **Puerto del** , puede especificar el número de puerto del servidor web en el que ejecuta WordPress. El valor predeterminado es 80.

e) En **DocumentRoot de la aplicación**, puede especificar la DocumentRoot de la aplicación PHP de WordPress. Utilice dos puntos para separar los registros. Para permitir que el agente busque todos los registros por usted, utilice el valor predeterminado ALL.

f) Guarde y cierre el archivo php_silent_config.txt y, a continuación, especifique:
dir_instalación/bin/php-agent.sh config *nombre_instancia dir_instalación*/samples/php_silent_config.txt
Donde *nombre_instancia* es el nombre que desea dar a la instancia y *dir_instalación* es el directorio de instalación de Agente de PHP. El directorio de instalación predeterminado es /opt/ibm/apm/agent.

g) Para iniciar el agente, especifique:
dir_instalación/bin/php-agent.sh start *nombre_instancia*

- Para configurar el agente mediante la ejecución del script y las respuestas a las solicitudes, siga estos pasos:

a) Escriba:
dir_instalación/bin/php-agent.sh config *nombre_instancia*
Donde *nombre_instancia* es el nombre que desea dar a la instancia y *dir_instalación* es el directorio de instalación de Agente de PHP.

b) Cuando se le solicite Editar valores de Monitoring Agent for PHP, especifique 1 para continuar.

c) Cuando se le solicite la Ubicación del binario de ejecución de PHP, pulse Intro para aceptar la ubicación predeterminada o especifique su propia ubicación.

d) Cuando se le solicite la Ubicación del archivo INI de PHP, pulse Intro para aceptar la ubicación predeterminada o especificar su propia ubicación.

e) Cuando se le solicite el Puerto del servidor web, pulse Intro para aceptar el puerto predeterminado o especifique un número de puerto diferente.

f) Cuando se le solicite la DocumentRoot de aplicación, pulse Intro para aceptar el valor predeterminado o especifique la DocumentRoot de la aplicación WordPress de PHP. Utilice dos puntos para separar los registros.

g) Para iniciar el agente, especifique:
dir_instalación/bin/php-agent.sh start *nombre_instancia*

Resultados
El agente solo evalúa el rendimiento de las peticiones PHP en aplicaciones WordPress. No se evalúan las cargas de CSS y JS. El agente no utiliza argumentos de URL para identificar los URL.

Qué hacer a continuación

Puede verificar que los datos de Agente de PHP se muestran en la Consola de Cloud APM.

Debe asegurarse de que el plugin de WordPress del agente esté activado. Para asegurar la activación, siga los pasos siguientes:

1. En un navegador web, escriba el siguiente URL: http://*nombrehost*:*puerto*/wp-admin/.
2. Acceda a la página de administración yendo a **Plugins** > **Plugins instalados**.
3. Asegúrese de que el plugin de Agente de PHP esté activado. El plugin de Agente de PHP aparece listado como **WordPress Agent**. Normalmente el plugin ya está activado. Si no estuviera ya activado, pulse en **Activar**.

Configuración de la supervisión de PostgreSQL

Debe configurar el Monitoring Agent for PostgreSQL para que el agente pueda recopilar datos de la base de datos de PostgreSQL que se está supervisando.

Antes de empezar

Debe instalar el controlador JDBC de PostgreSQL antes de instalar este agente. La vía de acceso a este controlador es necesaria durante la configuración del agente.

El controlador JDBC tipo 4 es la nueva versión y por lo tanto preferible. El usuario puede instalar el subtipo de la versión 4 de JDBC según la versión de JDK utilizada por el agente. Para obtener más información acerca de la correlación de la versión de JDBC con la versión de JDK, consulte https://jdbc.postgresql.org/download.html.

Algunos de los atributos recopilados por el agente se basan en la extensión `pg_stat_statements`. Para añadir `pg_stat_statements`, instale primero el paquete `postgresql-contrib`. Debe modificar el archivo de configuración `postgresql.conf` para que el servidor PostgreSQL cargue la extensión `pg_stat_statements`.

1. Abra el archivo `postgresql.conf` en un editor de texto y actualice la línea `shared_preload_libraries`:

   ```
   shared_preload_libraries = 'pg_stat_statements'
   pg_stat_statements.track_utility = false
   ```

   Estos cambios son necesarios para supervisar las sentencias SQL, excepto los mandatos de programa de utilidad.

   Nota: El estado de `pg_stat_statements.track_utility` sólo lo establece o modifica un superusuario.
2. Reinicie el servidor PostgreSQL tras actualizar y guardar `postgresql.conf`.
3. Ejecute el siguiente mandato SQL utilizando psql, que se debe conectar a la misma base de datos que se proporcionaría posteriormente en la configuración del agente para la conectividad JDBC:

   ```
   create extension pg_stat_statements;
   select pg_stat_statements_reset();
   ```

   Nota: El mandato `create extension` y la función `pg_stat_statements_reset()` sólo las puede ejecutar un superusuario.

   La vista `pg_stat_statements` debe estar habilitada para la base de datos específica. Para obtener más información, consulte https://www.postgresql.org/docs/9.6/static/pgstatstatements.html.

El archivo `pg_hba.conf` es el archivo de base de datos PostgreSQL que contiene los valores de autenticación. Cuando el valor del parámetro `auth-method` está establecido en `ident` en el archivo `pg_hba.conf`, el Agente de PostgreSQL no se puede conectar a la base de datos PostgreSQL. Asegúrese de que son correctos los valores de autenticación del parámetro `auth-method`. Por ejemplo, puede establecer estos valores para el parámetro `auth-method`: `md5`, `trust` o `password`.

Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de PostgreSQL.

Acerca de esta tarea

El Agente de PostgreSQL es un agente de varias instancias; debe crear la primera instancia e iniciar el agente de forma manual. El nombre de sistema gestionado incluye el nombre de instancia que especifique, por ejemplo, *nombre_instancia*:*nombre_host*:*pc*, donde *pc* es el código de producto de dos caracteres. El nombre de sistema gestionado está limitado a 32 caracteres. El nombre de instancia que especifique está limitado a 28 caracteres menos la longitud del nombre de host. Por ejemplo, si especifica `PostgreSQL2` como nombre de instancia, el nombre de sistema gestionado será `PostgreSQL2:nombrehost:PN`.

Importante: Si especifica un nombre de instancia largo, el nombre de sistema gestionado queda truncado y el código de agente no se visualiza correctamente.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte “Historial de cambios” en la página 52.

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte “Inicio de la Consola de Cloud APM” en la página 1009.

Configuración del agente en sistemas Windows

Puede utilizar la ventana de IBM Cloud Application Performance Management para configurar el agente en sistemas Windows.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en **Monitoring Agent for PostgreSQL** y luego pulse **Configurar agente**.
3. En el campo **Especificar un nombre de instancia exclusivo**, escriba el nombre de la instancia del agente y pulse **Aceptar**.
4. En la ventana **Monitoring Agent for PostgreSQL**, complete estos pasos:
   a. En el campo **Dirección IP**, especifique la dirección IP del servidor PostgreSQL que desee supervisar de forma remota. Si el agente se instala en el servidor a supervisar, retenga el valor predeterminado.

      Nota:

      Para la supervisión remota, los datos de **CPU actual utilizada (%)** y **Memoria física utilizada (MB)** no estarán disponibles en el panel de instrumentos. Estos widgets mostrarán **N/A**.
   b. En el campo **Nombre de base de datos de JDBC** , especifique un nombre de base de datos para cambiar el nombre de base de datos predeterminado `postgres`.
   c. En el campo **Nombre de usuario de JDBC**, especifique un nombre de usuario para cambiar el nombre predeterminado `postgres`.
   d. En el campo **Contraseña de JDBC**, escriba la contraseña de usuario de JDBC.
   e. En el campo **Confirmar contraseña de JBDC**, vuelva a especificar la contraseña.
   f. En el campo **Número de puerto JDBC**, especifique un número de puerto para cambiar el número de puerto predeterminado 5432.
   g. En el campo **Archivo JAR de JDBC**, especifique la vía de acceso del conector PostgreSQL para el archivo JAR Java y pulse **Siguiente**.
   h. En el campo **Nivel de rastreo de Java**, especifique el nivel de rastreo de acuerdo con las instrucciones del soporte de IBM. El nivel de rastreo predeterminado es `Error`.
   i. Pulse **Aceptar**. La instancia de agente se visualizará en la ventana IBM Performance Management.
5. Pulse la instancia de **Monitoring Agent for PostgreSQL** con el botón derecho del ratón y pulse **Iniciar**.

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información acerca de cómo usar la consola, consulte “Inicio de la Consola de Cloud APM” en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente en sistemas Linux

Para configurar el agente en sistemas operativos Linux, debe ejecutar el script y responder a las solicitudes.

Procedimiento

1. En la línea de mandatos, entre el siguiente mandato:
   dir_instalación/bin/postgresql-agent.sh config *nombre_instancia*
2. Cuando se le solicite editar el agente para los valores de PostgreSQL, especifique 1 para continuar.
3. Cuando se le solicite que especifique un valor para los parámetros siguientes, presione la tecla Intro para aceptar el valor predeterminado o especifique otro valor y presione la tecla Intro:
   - Dirección IP

     Nota:

     Especifique la dirección IP de un servidor PostgreSQL que desee supervisar de forma remota. Si el agente se instala en el servidor a supervisar, retenga el valor predeterminado.

     Para la supervisión remota, los datos de **CPU actual utilizada (%)** y **Memoria física utilizada (MB)** no estarán disponibles en el panel de instrumentos. Estos widgets mostrarán **N/A**.
   - Nombre de base de datos de JDBC
   - Nombre de usuario de JDBC
   - Contraseña de JDBC
   - Número de puerto de JDBC
   - Archivo .jar de JDBC

   Importante: La versión del archivo .jar de JDBC debe ser la misma que la versión de la base de datos PostgreSQL que se va a supervisar.
4. Cuando se le solicite que especifique un valor para el parámetro `Nivel de rastreo de Java`, introduzca 2 para aceptar el valor predeterminado o especifique el nivel de rastreo de acuerdo con las instrucciones del soporte de IBM.
5. Ejecute el mandato siguiente para iniciar el agente:

   ```
   dir_instalación/bin/postgresql-agent.sh
   start nombre_instancia
   ```

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

Puede utilizar el archivo de respuestas silencioso para configurar el Agente de PostgreSQL en sistemas Linux y Windows. Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

- Para configurar el agente mediante la edición del archivo de respuestas silencioso y la ejecución del script sin responder a las solicitudes, siga estos pasos:

  1. En un editor de texto, abra el archivo de respuestas silencioso que está disponible en esta vía de acceso: *dir_instalación*/samples/postgresql_silent_config.txt donde *dir_instalación* es el directorio de instalación de Agente de PostgreSQL. El directorio de instalación predeterminado es /opt/ibm/apm/agent.
  2. Para editar el archivo de configuración silenciosa, siga estos pasos:
     a. Para el parámetro **Dirección IP**, especifique la dirección IP de un servidor PostgreSQL que desee supervisar de forma remota. Si el agente se instala en el servidor a supervisar, retenga el valor predeterminado.

        Nota:

        Para la supervisión remota, los datos de **CPU actual utilizada (%)** y **Memoria física utilizada (MB)** no estarán disponibles en el panel de instrumentos. Estos widgets mostrarán **N/A**.
     b. Para el parámetro **Nombre de base de datos de JDBC**, especifique un nombre de base de datos para cambiar el nombre de base de datos predeterminado de postgres.
     c. Para el parámetro **Nombre de usuario de JDBC**, especifique un nombre de usuario para cambiar el nombre predeterminado de postgres.
     d. Para el parámetro **Contraseña de JDBC**, especifique la contraseña de usuario de JDBC.
     e. Para el **Número de puerto de JDBC**, especifique un número de puerto para cambiar el número de puerto predeterminado de 5432.
     f. Para el parámetro **archivo jar de JDBC**, especifique la vía de acceso del conector PostgreSQL para el archivo JAR Java si la vía de acceso predeterminada es incorrecta. La vía de acceso predeterminada del archivo JAR Java es:

        /opt/PostgreSQL/lib/postgresql-9.3-1100.jdbc4.jar

        Importante: La versión del archivo .jar de JDBC debe ser compatible con la versión de la base de datos PostgreSQL que se va a supervisar.
     g. Para el parámetro **Nivel de rastreo de Java**, especifique el nivel de rastreo de acuerdo con las instrucciones del soporte de IBM. El nivel de rastreo predeterminado es Error.
  3. Guarde y cierre el archivo de respuestas silencioso y ejecute el mandato siguiente:

     ```
     dir_instalación/bin/postgresql-agent.sh config
     nombre_instancia
     dir_instalación/samples/postgresql_silent_config.txt
     ```

     Donde *nombre_instancia* es el nombre que desea dar a la instancia.
  4. Para iniciar el agente, especifique el mandato siguiente:

     ```
     dir_instalación/bin/postgresql-agent.sh
     start nombre_instancia
     ```

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración de la supervisión de Python

Se pueden supervisar las aplicaciones Python locales y de IBM Cloud. Siga los pasos de configuración correspondientes en función del tipo de aplicación.

Acerca de esta tarea

Configure el Recopilador de datos de Python para supervisar las aplicaciones Python locales y de IBM Cloud.

Procedimiento

- Configure el recopilador de datos para supervisar aplicaciones de IBM Cloud.
  a) Configure el recopilador de datos de Python para recopilar y enviar datos de aplicaciones de IBM Cloud. Para obtener instrucciones, consulte "Configuración del recopilador de datos de Python para aplicaciones IBM Cloud" en la página 695.
  b) Opcional: Personalice las prestaciones de supervisión del Recopilador de datos de Python. Para obtener más información, consulte "Personalización del Recopilador de datos de Python para aplicaciones IBM Cloud" en la página 696.
- Configure el recopilador de datos para supervisar aplicaciones locales.
  a) Configure el recopilador de datos para recopilar y enviar datos al Servidor de Cloud APM. Para obtener instrucciones, consulte "Configuración del Recopilador de datos de Python para aplicaciones locales" en la página 701.
  b) Opcional: Personalice las prestaciones de supervisión del Recopilador de datos de Python. Para obtener más información, consulte "Personalización del Recopilador de datos de Python para aplicaciones locales" en la página 702.

Configuración del recopilador de datos de Python para aplicaciones IBM Cloud

Para recopilar información sobre aplicaciones Python en IBM Cloud, debe configurar el recopilador de datos de Python.

Antes de empezar

1. Asegúrese de que las aplicaciones Python que desea supervisar tengan nombres exclusivos. El Recopilador de datos de Python maneja dos aplicaciones diferentes con el mismo nombre que una aplicación, lo cual puede causar problemas de visualización de datos en la Consola de Cloud APM.
2. Descargue el paquete de recopilador de datos del sitio web de IBM Marketplace. Para obtener instrucciones detalladas, consulte "Descarga de los agentes y recopiladores de datos" en la página 107.

Acerca de esta tarea

Para configurar el recopilador de datos, primero debe desplegar un servidor de paquetes pypi, y luego instalar el recopilador de datos en una aplicación Python Django.

Procedimiento

1. Extraiga los archivos del paquete del recopilador de datos. El paquete `python_datacollector_8.1.4.0.tgz` está incluido en el directorio extraído.
2. Extraiga el paquete `python_datacollector_8.1.4.0.tgz`, por ejemplo, ejecutando el mandato siguiente:

   ```
   tar -zxf python_datacollector_8.1.4.0.tgz
   ```

3. Busque el archivo `manifest.yml` del servidor de paquetes en el directorio extraído y defina el dominio, host y nombre de este archivo como se muestra en el ejemplo siguiente:

```
domain: mybluemix.net
name: pythondc
host: pythondc
```

Recuerde: los valores *host* y *name* deben ser iguales y exclusivos.

4. Desde el directorio `python_dc`, envíe la aplicación `pythondc` a IBM Cloud ejecutando el mandato siguiente:

```
cf push
```

5. En el archivo `requirements.txt` de la aplicación Python, añada las líneas siguientes:

```
cryptography==1.9.0
--extra-index-url https://<nombre_y_dominio_su_host>/python-dc-repos/simple/
ibm_python_dc
```

6. En el archivo `settings.py` de la aplicación Python, añada `ibm_python_dc.kpg_plugin.ResourceMiddleware` al principio de la sección `MIDDLEWARE_CLASSES`, por ejemplo:

```
MIDDLEWARE_CLASSES = (
    "ibm_python_dc.kpg_plugin.ResourceMiddleware",
    "mezzanine.core.middleware.UpdateCacheMiddleware",
    'django.contrib.sessions.middleware.SessionMiddleware',
    'django.middleware.common.CommonMiddleware',
```

7. En el directorio que contiene el archivo `manifest.yml` de la aplicación Python ejecute el mandato siguiente:

```
cf push
```

Consejo: Para obtener un archivo `manifest.yml` de muestra, consulte "Ejemplo de archivo manifest.yml" en la página 196.

Resultados
El recopilador de datos se ha configurado y está conectado al Servidor de Cloud APM.

Qué hacer a continuación

Puede verificar que los datos de la aplicación IBM Cloud se visualizan en la Consola de Cloud APM. Para obtener instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte Inicio de la consola de Cloud APM. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte Gestión de aplicaciones.

Personalización del Recopilador de datos de Python para aplicaciones IBM Cloud
Puede añadir variables de entorno en la interfaz de usuario (IU) de IBM Cloudpara personalizar la supervisión de la aplicación IBM Cloud. Utilice la información siguiente para añadir las variables según sus necesidades.

Variables de entorno definidas por el usuario para el Recopilador de datos de Python

Puede utilizar la información de la tabla siguiente para personalizar la supervisión de Python en IBM Cloud.

Tabla 192. Variables de entorno definidas por el usuario soportadas para la supervisión de Python en IBM Cloud

Nombre de variable	Importancia	Valor	Descripción
APM_BM_GATEWAY_URL	Opcional	• https://*<ip o nombre de host del servidor>*:443 • http://*<ip o nombre de host del servidor>*:80	El URL de pasarela del servidor local de destino.
APM_KEYFILE_PSWD	Opcional	Contraseña cifrada del archivo de claves	La contraseña del archivo de claves cifrada que se empareja con el archivo de claves. Si es usuario de Linux, puede utilizar el mandato `echo -n <contraseña de archivo de claves> | base64` para cifrar la contraseña. **Nota:** establezca esta variable sólo cuando haya configurado la pasarela para utilizar HTTPS.
APM_KEYFILE_URL	Opcional	http://*<servidor http alojado>*:*<puerto>*/keyfile.p12	El URL utilizado para descargar el archivo de claves. **Nota:** establezca esta variable sólo cuando haya configurado la pasarela para utilizar HTTPS.
KPG_ENABLE_DEEPDIVE	Opcional	• False • True	Habilita o inhabilita la recopilación de datos de diagnóstico. • True: el valor predeterminado. Si establece esta variable en `True`, se recopilan datos de diagnóstico. • False: si establece esta variable en `False`, no se recopilan datos de diagnóstico. Si no establece esta variable, se recopilan datos de diagnóstico.
KPG_DD_CONFIG_FILE	Opcional	Nombre del archivo de configuración de supervisión de diagnósticos.	Nombre del archivo de configuración de supervisión de diagnósticos. El nombre de archivo predeterminado es `kpg_dd_config.xml`. **Nota:** después de personalizar los valores de este archivo, debe colocarlo en el directorio raíz de la aplicación. Si no establece esta variable, se utilizará el archivo de configuración predeterminado `kpg_dd_config.xml` del paquete de recopiladores de datos.

Tabla 192. Variables de entorno definidas por el usuario soportadas para la supervisión de Python en IBM Cloud (continuación)

Nombre de variable	Importancia	Valor	Descripción
KPG_DD_APP_PATH	Opcional	Vía de acceso a la aplicación Python.	La vía de acceso a la aplicación de Python o el módulo para el que el recopilador de datos recopila datos de diagnóstico. Separe las vías de acceso de diferentes aplicaciones Python y módulos que desee supervisar con signos de punto y coma `;`. Si no establece esta variable, el recopilador de datos recopila datos para las solicitudes y módulos utilizados por la aplicación. Los datos de solicitudes de la biblioteca de Python no se recopilan.
KPG_DD_SECURITY_FILTER	Opcional	• True • False	• True: el valor predeterminado. Si establece esta variable en `True`, los valores (como por ejemplo las contraseñas) estarán enmascarados en las sentencias SQL y los parámetros no se visualizarán en el widget de grupo **Contexto de solicitud**. • Falso: si establece esta variable en `False`, los valores de las sentencias SQL no estarán enmascarados y los parámetros se visualizarán en el widget de grupo **Contexto de solicitud**. Si no establece esta variable, los valores (como la contraseñas) estarán enmascarados en las sentencias SQL y los parámetros no se visualizarán en el widget de grupo **Contexto de solicitud**.

Tabla 192. Variables de entorno definidas por el usuario soportadas para la supervisión de Python en IBM Cloud (continuación)

Nombre de variable	Importancia	Valor	Descripción
KPG_GC_STATS	Opcional	True	Todas las funciones de estadísticas de recogida de basura de python están habilitados. Cuando se establece este valor en `True`, es igual a ejecutar el mandato siguiente: `gc.set_debug(gc.DEBUG_STATS | gc.DEBUG_COLLECTABLE | gc.DEBUG_UNCOLLECTABLE | gc.DEBUG_INSTANCES | gc.DEBUG_OBJECTS )` Para inhabilitar KPG_GC_STATS, suprima esta variable de entorno. No la establezca en `False`. **Nota:** nunca establezca `KPG_SAVE_ALL=True` en el entorno de producción habitual. Es sólo para la modalidad de depuración. Asegúrese de que se asigna suficiente memoria a la aplicación.
KPG_LOG_LEVEL	Opcional	• DEBUG • ERROR • INFO	• DEBUG: sólo se anota información de depuración útil en el registro, por ejemplo, datos recopilados, datos que se envían al servidor y la respuesta del servidor. • ERROR: sólo se anota información sobre excepciones y situaciones inesperadas en el registro. • INFO: se anota en el registro la información de resumen sobre el recopilador de datos para que el usuario sepa qué se está haciendo.
KPG_LOG_TOCONSOLE	Opcional	• Y • True • Cualquier otro valor que no sea `False`	El registro se refleja en la consola y el usuario puede verlo ejecutando el mandato **`cf logs <nombre_aplicación>`**.

Tabla 192. Variables de entorno definidas por el usuario soportadas para la supervisión de Python en IBM Cloud (continuación)

Nombre de variable	Importancia	Valor	Descripción
KPG_SAVE_ALL	Opcional	True	Todos los objetos no referenciados se guardan en `gc.garbage`, y debe borrarse `gc.garbage` cada minuto (el recopilador de datos lo borra automáticamente). Si el valor se establece en `True`, es igual a ejecutar el mandato siguiente: `gc.set_debug(gc.SAVE_ALL)` Para inhabilitar KPG_SAVE_ALL, suprima esta variable de entorno. No la establezca en `False`. **Nota:** nunca establezca `KPG_SAVE_ALL=True` en el entorno de producción habitual. Es sólo para la modalidad de depuración. Asegúrese de que se asigna suficiente memoria a la aplicación.

Desconfiguración del Recopilador de datos de Python para aplicaciones de IBM Cloud
Si no necesita supervisar el entorno de Python o si desea actualizar el Recopilador de datos de Python, primero debe desconfigurar varios valores del Recopilador de datos de Python.

Procedimiento

1. Vaya al directorio de inicio de la aplicación Python.
2. Elimine las líneas siguientes del archivo `requirements.txt` de la aplicación:

   ```
   --extra-index-url https://<nombre_y_dominio_su_host>/python_dc/static/python-dc-repos/simple/
   ibm-python-dc
   ```

3. En el archivo `settings.py`, elimine la línea siguiente de la sección `MIDDLEWARE_CLASSES`:

   ```
   ibm_python_dc.kpg_plugin.ResourceMiddleware
   ```

4. Ejecute el mandato siguiente para volver a enviar la aplicación para que los cambios entren en vigor:

   ```
   cf push
   ```

Resultados
Ha desconfigurado satisfactoriamente el Recopilador de datos de Python.

Qué hacer a continuación
Tras desconfigurar el recopilador de datos, la Consola de Cloud APM continúa mostrando el recopilador de datos en cualquier aplicación a la que haya añadido el recopilador de datos. La Consola de Cloud APM mostrará que no hay datos disponibles para la aplicación y no indicará que el recopilador de datos está fuera de línea. Para obtener información sobre cómo eliminar el recopilador de datos de aplicaciones y de grupos de recursos, consulte "Eliminación de recopiladores de datos de Consola de Cloud APM" en la página 196.

Configuración del Recopilador de datos de Python para aplicaciones locales

Para recopilar información sobre aplicaciones de Python ejecutadas en el entorno local, debe configurar el Recopilador de datos de Python.

Antes de empezar

1. Asegúrese de que las aplicaciones Python que desea supervisar tengan nombres exclusivos. El Recopilador de datos de Python maneja dos aplicaciones diferentes con el mismo nombre que una aplicación, lo cual puede causar problemas de visualización de datos en la Consola de Cloud APM.
2. Descargue el paquete de recopilador de datos del sitio web de IBM Marketplace. Para obtener instrucciones detalladas, consulte "Descarga de los agentes y recopiladores de datos" en la página 107.

Acerca de esta tarea

El paquete de recopilador de datos está preconfigurado con un archivo `global.environment` preconfigurado y un archivo `keyfile.p12` que se copia en la carpeta `etc`. Como resultado, el recopilador de datos se conecta automáticamente al Servidor de Cloud APM.

El procedimiento siguiente configura el recopilador de datos dentro de la aplicación Python con los valores predeterminados. Para personalizar la configuración del recopilador de datos, utilice las variables de entorno de los archivos de configuración del recopilador de datos. Para obtener más información, consulte "Personalización del Recopilador de datos de Python para aplicaciones locales" en la página 702.

Procedimiento

1. Extraiga los archivos del paquete del recopilador de datos. El paquete `python_datacollector_8.1.4.0.tgz` está incluido en el directorio extraído.
2. Extraiga los archivos del paquete del recopilador de datos, por ejemplo ejecutando el mandato siguiente:

   ```
   tar -zxf python_datacollector_8.1.4.0.tgz
   ```

3. En el directorio `python_dc`, ejecute el mandato siguiente:

   ```
   python server.py
   ```

4. Ejecute el mandato siguiente:

   ```
   pip install ibm_python_dc --extra-index-url http://nombre host o ip:8000/
   python-dc-repos/simple/ --trusted-host nombre host o ip
   ```

   siendo *nombre host o ip* el nombre o la dirección IP del host para ejecutar el repositorio recopilador de datos Python.

   Importante: Utilice el nombre o la dirección IP para especificar el host para el URL y para el host de confianza en este mandato. Por ejemplo, si especifica el host utilizando la dirección IP y ésta es `9.42.36.180`, el mandato es el siguiente:

   ```
   pip install ibm_python_dc --extra-index-url http://9.42.36.180:8000/
   python-dc-repos/simple/ --trusted-host 9.42.36.180
   ```

5. En el archivo `settings.py` de la aplicación Python, añada `ibm_python_dc.kpg_plugin.ResourceMiddleware` a la sección `MIDDLEWARE_CLASSES` en el formato del ejemplo siguiente:

   ```
   MIDDLEWARE_CLASSES = (
       "ibm_python_dc.kpg_plugin.ResourceMiddleware",
       "mezzanine.core.middleware.UpdateCacheMiddleware",
       'django.contrib.sessions.middleware.SessionMiddleware',
       'django.middleware.common.CommonMiddleware',
   ```

Resultados
El recopilador de datos se ha configurado con los valores predeterminados y se ha conectado al Servidor de Cloud APM.

Qué hacer a continuación
Ahora puede iniciar la sesión en el Servidor de Cloud APM para ver los datos de supervisión.

Recuerde: después de añadir la aplicación Python a la Consola de Cloud APM, puede ver sus datos de supervisión en el componente denominado aplicación de Tiempo de ejecución de Python.

Para obtener instrucciones sobre cómo iniciar el Servidor de Cloud APM, consulte Inicio de la consola de Cloud APM. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte Gestión de aplicaciones.

Personalización del Recopilador de datos de Python para aplicaciones locales
Modificando los archivos del paquete de recopilador de datos, puede establecer las variables de entorno para personalizar la supervisión de la aplicación Python.

Se suministran dos archivos para personalizar los valores del recopilador de datos, `global.environment` y `config.properties`. Después de cambiar los valores de estos archivos, reinicie la aplicación Python para que el cambio entre en vigor.

Modificando el archivo `global.environment`, puede personalizar la conexión entre el recopilador de datos y el Servidor de Cloud APM. Si desea utilizar otro Servidor de Cloud APM en lugar del predeterminado, o el archivo de claves o su contraseña han cambiado, modifique el Servidor de Cloud APM para volver a conectar el recopilador de datos al Servidor de Cloud APM.

Modificando el archivo `config.properties`, puede personalizar los comportamientos del recopilador de datos según sus necesidades, como por ejemplo habilitar o inhabilitar el rastreo de método.

El archivo de configuración `global.environment`

La Tabla 193 en la página 702 muestra las variables de entorno que puede establecer en el archivo de configuración `global.environment` y las descripciones asociadas. Puede encontrar el archivo `global.environment` en la carpeta `etc` donde está instalado el Recopilador de datos de Python, por ejemplo, en el directorio `/root/.pyenv/versions/3.5.2/lib/python3.5/site-packages/ibm_python_dc/etc`.

Tabla 193. Variables de entorno soportadas en el archivo `global.environment`

Nombre de variable	Importancia	Valor	Descripción
APM_BM_GATEWAY_URL	Opcional	• https://*<ip o nombre de host del servidor>*:443 • http://*<ip o nombre de host del servidor>*:80	El URL de pasarela del servidor local de destino.
APM_KEYFILE_PSWD	Opcional	Contraseña del archivo de claves	La contraseña del archivo de claves que se empareja con el archivo de claves. **Nota:** establezca esta variable sólo cuando haya configurado la pasarela para utilizar HTTPS.

Tabla 193. Variables de entorno soportadas en el archivo `global.environment` (continuación)			
Nombre de variable	**Importancia**	**Valor**	**Descripción**
APM_KEYFILE_URL	Opcional	http://*<servidor http alojado>*:*<puerto>*/keyfile.p12	El URL utilizado para descargar el archivo de claves. **Nota:** establezca esta variable sólo cuando haya configurado la pasarela para utilizar HTTPS.

El archivo `config.properties`

La Tabla 194 en la página 703 muestra las variables de entorno que puede establecer en los archivos de configuración `config.properties` y la descripción asociada. Puede encontrar el archivo `config.properties` en el directorio de instalación del Recopilador de datos de Python, por ejemplo el directorio `/root/.pyenv/versions/3.5.2/lib/python3.5/site-packages/ibm_python_dc`.

Tabla 194. Variables de entorno soportadas en el archivo `config.properties`			
Nombre de variable	**Importancia**	**Valor**	**Descripción**
KPG_ENABLE_DEEPDIVE	Opcional	• False • True	• False: el valor predeterminado. Si establece esta variable en `False`, no se recopilarán datos de diagnóstico. • True: si establece esta variable en `True`, se recopilarán datos de diagnóstico. El nivel predeterminado es `True`. Si no establece esta variable, no se recopilarán datos de diagnóstico.
KPG_DD_CONFIG_FILE	Opcional	Nombre del archivo de configuración de supervisión de diagnósticos.	Nombre del archivo de configuración de supervisión de diagnósticos. El nombre de archivo predeterminado es `kpg_dd_config.xml`. **Nota:** después de personalizar los valores de este archivo, debe colocarlo en el directorio raíz de la aplicación. Si no establece esta variable, se utilizará el archivo de configuración predeterminado `kpg_dd_config.xml` del paquete de recopiladores de datos.

Tabla 194. Variables de entorno soportadas en el archivo `config.properties` (continuación)			
Nombre de variable	**Importancia**	**Valor**	**Descripción**
KPG_DD_APP_PATH	Opcional	Vía de acceso a la aplicación Python.	La vía de acceso a la aplicación de Python o el módulo para el que el recopilador de datos recopila datos de diagnóstico. Separe las vías de acceso de diferentes aplicaciones Python y módulos que desee supervisar con signos de punto y coma `;`. Si no establece esta variable, el recopilador de datos recopilará datos para las solicitudes y módulos utilizados por la aplicación. Los datos de solicitudes de la biblioteca de Python no se recopilarán.
KPG_DD_SECURITY_FILTER	Opcional	• True • False	• True: el valor predeterminado. Si establece esta variable en `True`, los valores (como por ejemplo las contraseñas) estarán enmascarados en las sentencias SQL y los parámetros no se visualizarán en el widget de grupo **Contexto de solicitud**. • False: si establece esta variable en `False`, los valores de las sentencias SQL no estarán enmascarados y los parámetros se visualizarán en el widget de grupo **Contexto de solicitud**. Si no establece esta variable, los valores (como la contraseñas) estarán enmascarados en las sentencias SQL y los parámetros no se visualizarán en el widget de grupo **Contexto de solicitud**.

Tabla 194. Variables de entorno soportadas en el archivo `config.properties` (continuación)

Nombre de variable	Importancia	Valor	Descripción
KPG_GC_STATS	Opcional	True	Todas las funciones de estadísticas de recogida de basura de python están habilitados. Cuando se establece este valor en `True`, es igual a ejecutar el mandato siguiente: `gc.set_debug(gc.DEBUG_STATS | gc.DEBUG_COLLECTABLE | gc.DEBUG_UNCOLLECTABLE | gc.DEBUG_INSTANCES | gc.DEBUG_OBJECTS )` Para inhabilitar KPG_GC_STATS, suprima esta variable de entorno. No la establezca en `False`. El valor predeterminado es `True`. **Nota:** nunca establezca KPG_GC_STATS=`True` en el entorno de producto habitual. Es sólo para la modalidad de depuración. Asegúrese también de que se asigna suficiente memoria a la aplicación.
KPG_LOG_LEVEL	Opcional	• DEBUG • ERROR • INFO	• DEBUG: sólo se anotará información de depuración útil en el registro, por ejemplo, datos recopilados, datos que se envían al servidor y la respuesta del servidor. • ERROR: sólo se anotará información sobre excepciones y situaciones muy inesperadas en el registro. • INFO: se anotará en el registro la información de resumen sobre el recopilador de datos para que el usuario sepa qué se está haciendo. El valor predeterminado es ERROR.
KPG_LOG_TOCONSOLE	Opcional	• Y • True • Cualquier otro valor que no sea `False`	El registro se reflejará en la consola y el usuario podrá verlo ejecutando el mandato **`cf logs <nombre_aplicación>`**. El valor predeterminado es `True`.

Tabla 194. Variables de entorno soportadas en el archivo `config.properties` (continuación)

Nombre de variable	Importancia	Valor	Descripción
KPG_SAVE_ALL	Opcional	True	Todos los objetos no referenciados se guardarán en `gc.garbage`, y debe borrarse `gc.garbage` cada minuto (el recopilador de datos lo hace automáticamente). Si el valor se establece en `True`, es igual a ejecutar el mandato siguiente: `gc.set_debug(gc.SAVE_ALL)` Para inhabilitar KPG_SAVE_ALL, suprima esta variable de entorno. No la establezca en `False`. El valor predeterminado es `True`. **Nota:** nunca establezca `KPG_SAVE_ALL=True` en el entorno de producto habitual. Es sólo para la modalidad de depuración. Asegúrese también de que se asigna suficiente memoria a la aplicación.
APM_GW_PROXY_CONNECTION	Opcional	http://*<ip o nombre de host del servidor>*:port	El proxy HTTP o HTTPS que el recopilador de datos de Python utiliza para enviar datos de supervisión.

Desconfiguración del Recopilador de datos de Python para aplicaciones locales
Si no necesita supervisar el entorno de Python o si desea actualizar el Recopilador de datos de Python, primero debe desconfigurar varios valores del Recopilador de datos de Python.

Procedimiento

1. Vaya al directorio de inicio de la aplicación Python.
2. Elimine las líneas siguientes del archivo `requirements.txt` de la aplicación:

   ```
   --extra-index-url https://<nombre_y_dominio_su_host>/python_dc/static/python-dc-repos/simple/
   ibm-python-dc
   ```

3. En el archivo `settings.py`, elimine la línea siguiente de la sección `MIDDLEWARE_CLASSES`:

   ```
   ibm_python_dc.kpg_plugin.ResourceMiddleware
   ```

4. Ejecute el mandato `pip uninstall ibm_python_dc` para desinstalar el Recopilador de datos de Python del tiempo de ejecución Python.

Resultados
Ha desconfigurado satisfactoriamente el Recopilador de datos de Python.

Qué hacer a continuación
Tras desconfigurar el recopilador de datos, la Consola de Cloud APM continúa mostrando el recopilador de datos en cualquier aplicación a la que haya añadido el recopilador de datos. La Consola de Cloud APM mostrará que no hay datos disponibles para la aplicación y no indicará que el recopilador de datos está fuera de línea. Para obtener información sobre cómo eliminar el recopilador de datos de aplicaciones y de

grupos de recursos, consulte “Eliminación de recopiladores de datos de Consola de Cloud APM” en la página 196.

Configuración de la supervisión de RabbitMQ

El Monitoring Agent for RabbitMQ supervisa el estado y el rendimiento de los recursos del clúster RabbitMQ, como por ejemplo los nodos, las colas y los canales del clúster. Debe configurar el Agente de RabbitMQ para que el agente pueda recopilar los datos de RabbitMQ.

Antes de empezar

- Revise los requisitos previos de hardware y software.
- Asegúrese de que el usuario de RabbitMQ, que se conecta al nodo, tiene permiso de lectura y de que el indicador de supervisión, administrador o gestión esté habilitado para este usuario.
- Asegúrese de que el plugin de gestión de RabbitMQ está habilitado en todos los nodos del clúster, ya que, si un nodo del clúster falla, el agente de RabbitMQ se conectará a un nodo igual que esté disponible en el clúster.

Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de RabbitMQ.

Acerca de esta tarea

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte “Historial de cambios” en la página 52.

El Agente de RabbitMQ es un agente de múltiple instancia. Deberá crear la primera instancia e iniciar el agente manualmente.

- Para configurar el agente en sistemas Windows, puede utilizar la ventana IBM Cloud Application Performance Management o el archivo de respuestas silencioso.
- Para configurar el agente en sistemas Linux, puede ejecutar el script y responder a las solicitudes, o utilizar el archivo de respuestas silencioso.

Configuración del agente en sistemas Windows

Puede utilizar la ventana de IBM Cloud Application Performance Management para configurar el agente en sistemas Windows.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en **Monitoring Agent for RabbitMQ** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar el agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar el agente de nuevo, pulse **Reconfigurar**.
3. En el campo **Especificar un nombre de instancia exclusivo**, escriba el nombre de la instancia del agente y pulse **Aceptar**.
4. En la ventana **Monitoring Agent for RabbitMQ**, especifique valores para los parámetros de configuración y a continuación pulse **Siguiente**.

   Para obtener información sobre los parámetros de configuración, consulte el tema siguiente: “Parámetros de configuración del agente” en la página 709

5. Pulse el botón derecho del ratón en la instancia de **Monitoring Agent for RabbitMQ** y pulse **Iniciar**.

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información acerca de cómo usar la consola, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente en sistemas Linux

Para configurar el agente en sistemas operativos Linux, debe ejecutar el script y responder a las solicitudes.

Procedimiento

1. En la línea de mandatos, especifique el mandato siguiente: *dir_instalación*/bin/rabbitmq.sh config *nombre_instancia*, donde *nombre_instancia* es el nombre que desea dar a la instancia:
2. Cuando se le solicite que proporcione un valor para los parámetros siguientes, presione la tecla Intro para aceptar el valor predeterminado o especifique un valor y luego pulse la tecla Intro:
   - Dirección IP
   - Nombre de usuario
   - Contraseña
   - Número de puerto
   - Directorio inicial de Java
   - Nivel de rastreo de Java

   Para obtener información sobre los parámetros de configuración, consulte el tema siguiente: "Parámetros de configuración del agente" en la página 709
3. Ejecute el mandato siguiente para iniciar el agente:

```
dir_instalación/bin/rabbitmq.sh start nombre_instancia
```

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea
Puede utilizar el archivo de respuestas silencioso para configurar el Agente de RabbitMQ en sistemas Linux y Windows. Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

1. Abra el archivo de respuestas silencioso que está disponible en esta vía de acceso: *dir_instalación*\samples\rabbitmq_silent_config.txt
2. En el archivo rabbitmq_silent_config.txt, especifique valores para todos los parámetros obligatorios. También puede modificar los valores predeterminados de otros parámetros.

   Para obtener información sobre los parámetros de configuración, consulte el tema siguiente: "Parámetros de configuración del agente" en la página 709
3. Guarde el archivo de respuestas y ejecute el mandato siguiente:

   Linux AIX *dir_instalación*/bin/rabbitmq-agent.sh config *dir_instalación*/samples/rabbitmq_silent_config.txt

   Windows *dir_instalación*/bin/rabbitmq-agent.bat config *dir_instalación*/samples/rabbitmq_silent_config.txt
4. Inicie el agente:

   Linux AIX Ejecute el mandato siguiente: *dir_instalación*\bin\rabbitmq-agent.sh start

   Windows Pulse el botón derecho del ratón en **Monitoring Agent for RabbitMQ** y, a continuación, pulse **Iniciar**.

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Parámetros de configuración del agente

Al configurar el Agente de RabbitMQ, puede cambiar el valor predeterminado de los parámetros, como el nombre de instancia y los certificados de validación SSL.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del Agente de RabbitMQ.

Tabla 195. Nombres y descripciones de los parámetros de configuración del Agente de RabbitMQ

Nombre de parámetro	Descripción	Campo obligatorio
Dirección IP	La dirección IP del nodo donde está instalada la aplicación RabbitMQ.	Sí
Nombre de usuario	El nombre de usuario de RabbitMQ.	Sí
Contraseña	La contraseña para conectarse a la interfaz de usuario de gestión de RabbitMQ.	Sí
Confirmar contraseña	La misma contraseña que ha especificado en el campo **Contraseña**.	Sí
Número de puerto	El número de puerto en el que el plug-in de gestión de RabbitMQ está habilitado. Utilice el número de puerto predeterminado 15672 o especifique otro número de puerto.	No
Directorio de inicio de Java	La vía de acceso donde está instalado el plug-in de Java. Utilice la vía de acceso predeterminada C:\Archivos de programa\IBM\Java50 o la vía de acceso del directorio en el que está instalado el plug-in java.	No

Tabla 195. Nombres y descripciones de los parámetros de configuración del Agente de RabbitMQ (continuación)		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Nivel de rastreo de Java	El nivel de rastreo del proveedor de Java. Los valores de nivel de rastreo válidos son los siguientes: • APAGADO • ERROR • WARN • INFO • DEBUG_MAX • TODOS	No

Configuración de la supervisión de tiempo de respuesta

El agente de Supervisión de tiempo de respuesta supervisa transacciones HTTP y HTTPS en el servidor HTTP. También se supervisan las transacciones de usuario basadas en navegador reales (temporizaciones de navegador).

El agente de Supervisión de tiempo de respuesta puede utilizarse para ver los siguientes niveles de información de supervisión:

Supervisión de transacciones HTTP y HTTPS
La supervisión de transacciones HTTP está disponible automáticamente cuando se instala el agente de Supervisión de tiempo de respuesta.

Dependiendo del tipo de servidor HTTP que éste supervisando, la supervisión de transacciones HTTPS puede estar automáticamente disponible o puede que deba configurarse manualmente. Para obtener más información, consulte “Supervisión de tiempo de respuestaComponentes” en la página 711.

La Supervisión de tiempo de respuesta también supervisa los datos relacionados con los recuentos de usuarios, los recuentos de sesiones y los dispositivos.

Los datos se presentan en el panel de instrumentos de Transacciones de usuario final en la hora local del usuario y también se utilizan en el widget Solicitudes y tiempo de respuesta.

Supervisión de transacciones de usuario final real (temporizaciones de navegador)
Dependiendo del tipo de servidor HTTP que éste supervisando, las temporizaciones basadas en navegador pueden estar disponibles automáticamente o puede que deban configurarse manualmente. Para obtener más información, consulte “Supervisión de tiempo de respuestaComponentes” en la página 711.

Las temporizaciones basadas en navegador se realizan mediante Inyección JavaScript.

Con la inyección JavaScript, puede ver más widgets y detalles dentro de los paneles de instrumentos Transacción de usuario final. La Inyección JavaScript garantiza que el tiempo de respuesta real del usuario final se recopile desde el navegador. Supervisa el rendimiento de páginas HTTP y objetos incluidos para páginas web servidas por el servidor HTTP. Están disponibles los siguientes detalles de transacción de usuario final real:

- Tiempo total del cliente en el widget Solicitudes y tiempo de respuesta de transacción
- Tiempo de respuesta para transacciones de tiempo de cliente en el widget Transacciones - 10 principales
- Desglose de tiempo de representación

Para obtener información sobre cómo configurar la inyección JavaScript, consulte “Inyección JavaScript” en la página 714.

Visualización de los paneles de instrumentos de transacciones

Vea datos de transacciones en Panel de instrumentos del rendimiento de aplicaciones.

En Panel de instrumentos del rendimiento de aplicaciones hay disponibles diversos widgets que le proporcionan información contextual sobre las transacciones.

Las *Solicitudes buenas* tienen un tiempo de respuesta inferior a 10 segundos. Las *Solicitudes lentas* tienen un tiempo de respuesta superior a 10 segundos. El valor de 10 segundos utilizado para determinar un tiempo de respuesta bueno vs. un tiempo de respuesta malo es configurable. Están disponibles los widgets siguientes:

- Widget de grupo Peor por usuario - 5 principales
- Widget de grupo Peor por dispositivo - 5 principales
- Widget de grupo Solicitudes y tiempo de respuesta
- Widget de grupo Transacciones - Principales 10
- Widget de grupo Solicitudes y tiempo de respuesta de transacción
- Widget de grupo Se ejecuta en
- Widget de grupo Subtransacciones
- Widget de grupo Instancias de transacciones
- Widget de grupo Usuarios por ubicación
- Widget de grupo Usuarios en la ubicación seleccionada
- Widget de grupo Sesiones de usuario en la ubicación seleccionada - 10 principales
- Widget de grupo Solicitud de usuario y tiempo de respuesta
- Widget de grupo Sesiones de usuario - 10 principales
- Widget de grupo Solicitudes de dispositivo y tiempo de respuesta
- Widget de grupo Sesión
- Widget de grupo Solicitudes de sesión
- Widget de grupo Instancias de sesión
- Widget de grupo Instancias de transacciones
- Panel de instrumentos Resumen de transacciones de middleware
- Panel de instrumentos Detalles de transacciones de middleware
- Umbrales de suceso para la supervisión de transacciones
- Datos agregados de interacciones
- Datos de agregados de transacciones
- Estado de transacción de WRT

Supervisión de tiempo de respuestaComponentes

La funcionalidad base del agente de Supervisión de tiempo de respuesta es:

- Supervisión de transacciones HTTP
- Supervisión de transacciones HTTPS
- Supervisión de temporizaciones basadas en navegador (mediante Inyección de JavaScript)

Para ver más descripciones detalladas de esta funcionalidad, consulte “Configuración de la supervisión de tiempo de respuesta ” en la página 710.

En función del tipo de servidor HTTP que esté supervisando, la funcionalidad base del agente de Supervisión de tiempo de respuesta se proporciona utilizando uno de los siguientes componentes:

Módulo de Tiempo de respuesta de IBM HTTP Server

El Módulo de Tiempo de respuesta de IBM HTTP Server sólo puede supervisar tipo de contenido http text/html, application/xml o application/json. (sin inyección de JavaScript)

Actualmente, el Módulo de Tiempo de respuesta de IBM HTTP Server no puede supervisar solicitudes comprimidas instrumentadas en javascript.

La inyección de Javascript de Módulo de Tiempo de respuesta de IBM HTTP Server sólo puede supervisar actualmente el tipo de contenido http text/html.

Analizador de paquetes

El Analizador de paquetes sólo puede supervisar el tipo de contenido text/html. El Analizador de paquetes puede supervisar solicitudes comprimidas en gzip.

Si está supervisando un servidor IBM HTTP Server o Apache HTTP Server en AIX o Linux, utilice el Módulo de Tiempo de respuesta de IBM HTTP Server. Es posible, pero no recomendable, utilizar el Analizador de paquetes. El Módulo de Tiempo de respuesta de IBM HTTP Server no está soportado en Windows. Utilice el Analizador de paquetes en un entorno Windows.

Si está supervisando cualquier otro servidor HTTP, utilice el Analizador de paquetes. El Analizador de paquetes está soportado en Windows, Linux y AIX.

Planificación de la instalación

Planifique la instalación del agente de Supervisión de tiempo de respuesta en función del sistema operativo y del tipo de servidor HTTP.

La funcionalidad base de Supervisión de tiempo de respuesta puede obtenerse utilizando uno de los siguientes componentes:

- Analizador de paquetes
- Módulo de Tiempo de respuesta de IBM HTTP Server

Determinará qué componente utilizar basándose en:

- El tipo de servidor HTTP en el que está instalando el agente de Supervisión de tiempo de respuesta.
- El sistema operativo en el que está instalado el servidor HTTP.

Las consideraciones para instalar el agente de Supervisión de tiempo de respuesta con el Analizador de paquetes son:

- El Analizador de paquetes está soportado en todos los sistemas operativos (Windows, Linux y AIX).
- El Analizador de paquetes supervisa transacciones HTTP en el puerto 80 para todos los sistemas operativos.
- La supervisión de transacciones HTTPS no es automática y debe configurarse manualmente. El agente de Supervisión de tiempo de respuesta requiere acceso a los certificados SSL para poder descifrar el tráfico SSL de los servidores HTTP. Para obtener más información, consulte “Supervisión de transacciones HTTPS” en la página 732.
- El Analizador de paquetes está soportado en todos los servidores HTTP, pero sólo es recomendable para Sun Java System Web Server y Microsoft Internet Information Services.
- AIX Linux Windows Para instalar el agente de Supervisión de tiempo de respuesta para que funcione con Analizador de paquetes en IBM HTTP Server o Apache HTTP Server, el servidor HTTP debe estar detenido. Al instalar el agente de Supervisión de tiempo de respuesta con el servidor HTTP detenido, el Analizador de paquetes se habilita automáticamente.
- AIX Linux Windows Aunque Analizador de paquetes puede configurarse para IBM HTTP Server o Apache HTTP Server, no es aconsejable; se recomienda Módulo de Tiempo de respuesta de IBM HTTP Server.
- Windows Es necesario WinPcap 4.1.3 para poder instalar el agente de Supervisión de tiempo de respuesta.

- Windows AIX Linux Si instala el agente de Supervisión de tiempo de respuesta en Sun Java System Web Server o Microsoft Internet Information Services, Analizador de paquetes se configura automáticamente.

Las consideraciones para instalar el agente de Supervisión de tiempo de respuesta con el Módulo de Tiempo de respuesta de IBM HTTP Server son:

- El Módulo de Tiempo de respuesta de IBM HTTP Server es un componente del Agente de HTTP Server. Debe instalar el Agente de HTTP Server antes que el agente de Supervisión de tiempo de respuesta o instalarlo simultáneamente. Para obtener más información, consulte "Módulo de Tiempo de respuesta de IBM HTTP Server" en la página 721.
- El Módulo de Tiempo de respuesta de IBM HTTP Server está soportado en todos los sistemas operativos (Windows, Linux y AIX). El Módulo de Tiempo de respuesta de IBM HTTP Server da soporte a IBM HTTP Server versión 7, 8 y 9.
- Instale el agente de Supervisión de tiempo de respuesta y el Agente de HTTP Server en la misma máquina.
- El Módulo de Tiempo de respuesta de IBM HTTP Server supervisa todos los puertos para detectar solicitudes HTTP y HTTPS en AIX, Linux y Windows.
- El Módulo de Tiempo de respuesta de IBM HTTP Server sólo está soportado para IBM HTTP Server o Apache HTTP Server.
- Ambos agentes se inician automáticamente, pero debe reiniciar el servidor HTTP.

La tabla siguiente describe los diferentes combinaciones de configuración automática del agente de Supervisión de tiempo de respuesta.

Tabla 196. Escenarios de configuración automática del agente de Supervisión de tiempo de respuesta

Combinaciones de servidor HTTP y sistema operativo	**Analizador de paquetes**	**Módulo de Tiempo de respuesta de IBM HTTP Server**
Sun Java System Web Server o Microsoft Internet Information Services en AIX o Linux	Automático	No soportado
Sun Java System Web Server o Microsoft Internet Information Services en Windows	Automático	No soportado
IBM HTTP Server o Apache HTTP Server en AIX, Linux o Windows	Automático si el servidor HTTP se ha detenido	Automático si el servidor HTTP está presente y configurado

Planificación de la configuración

La supervisión de HTTP se habilita automáticamente cuando se instala el agente de Supervisión de tiempo de respuesta. Dependiendo de su entorno, puede que sea necesario configurar manualmente HTTPS e Inyección JavaScript.

Supervisión de HTTP

La supervisión de transacciones HTTP se configura automáticamente para el Analizador de paquetes y el Módulo de Tiempo de respuesta de IBM HTTP Server, si se siguen las directrices de instalación. Consulte "Planificación de la instalación " en la página 712.

Supervisión de HTTPS

La supervisión de transacciones HTTPS se configura automáticamente para el Módulo de Tiempo de respuesta de IBM HTTP Server si sigue las directrices de instalación. Consulte "Planificación de la instalación " en la página 712.

la supervisión de transacciones HTTPS debe configurarse manualmente para el Analizador de paquetes. Para obtener más información, consulte “ Hoja de ruta del Analizador de paquetes” en la página 729.

Temporizaciones basadas en navegador (mediante Inyección de JavaScript)
Las temporizaciones basadas en navegador (utilizando Inyección JavaScript) se configuran automáticamente para el Módulo de Tiempo de respuesta de IBM HTTP Server.

Las temporizaciones basadas en navegador (utilizando Inyección JavaScript) deben configurarse manualmente para el Analizador de paquetes. Para obtener más información, consulte “ Hoja de ruta del Analizador de paquetes” en la página 729.

La tabla siguiente describe cómo se configura la funcionalidad básica para cada componente:

Tabla 197. Configuración de la funcionalidad básica

	Analizador de paquetes en Sun Java System Web Server o Microsoft Internet Information Services (Windows, Linux o AIX)	**Módulo de Tiempo de respuesta de IBM HTTP Server en IBM HTTP Server o Apache HTTP Server (Windows, Linux o AIX)**
Supervisión de transacciones HTTP	Habilitada automáticamente.	Habilitada automáticamente
Supervisión de transacciones HTTPS	Deben configurarse manualmente.	Habilitada automáticamente
Supervisión de transacciones de usuario final real (temporizaciones de navegador) mediante Instrumentación JavaScript	Deben configurarse manualmente.	Habilitada automáticamente

Inyección JavaScript

Puede personalizar los datos recopilados por el agente de Supervisión de tiempo de respuesta para visualizar en los paneles de instrumentos de Transacciones de usuario final.

Para garantizar una buena experiencia de usuario para una aplicación basada en la web, debe supervisar el rendimiento que es percibido por los usuarios reales. Esto significa supervisar en el nivel del navegador.

Para poder supervisar en el nivel de navegador, debe inyectar código de supervisión JavaScript en las páginas que desea supervisar. A continuación, este código recopilará datos para las temporizaciones del navegador en particular.

Esta operación se realiza utilizando inyección de JavaScript en las páginas web y objetos que desea supervisar. Dependiendo del tipo de servidor HTTP en el que haya instalado el agente de Supervisión de tiempo de respuesta, hay dos métodos que puede utilizar para recopilar información de tiempo de respuesta real de transacciones de usuario final.

- Si está utilizando un servidor IBM HTTP Server o un servidor HTTP Apache, utilice el Módulo de Tiempo de respuesta de IBM HTTP Server. El Módulo de Tiempo de respuesta de IBM HTTP Server realiza automáticamente la inyección de JavaScript. El Módulo de Tiempo de respuesta de IBM HTTP Server es un componente del Agente de HTTP Server. Se instala y configura como parte del Agente de HTTP Server. Para obtener más información, consulte “Módulo de Tiempo de respuesta de IBM HTTP Server” en la página 721.
- Si está utilizando cualquier otro servidor HTTP soportado, utilice el Analizador de paquetes. Con el Analizador de paquetes, debe instrumentar manualmente las páginas web para recopilar las

temporizaciones del navegador. Para obtener más información, consulte “Adición del componente de supervisión de JavaScript a la aplicación” en la página 730.

La tabla siguiente muestra las funciones que están disponibles en el Panel de instrumentos del rendimiento de aplicaciones si configura el entorno para el Analizador de paquetes o el Módulo de Tiempo de respuesta de IBM HTTP Server:

	Analizador de paquetes	**Módulo de Tiempo de respuesta de IBM HTTP Server**
10 principales transacciones	✓	✓
Tiempo de servidor	✓	✓
Desglose de tiempo de representación	—	✓
Subtransacciones AJAX	✓	✓
Datos de Temporización de recursos en tabla Subtransacciones	—	✓
Instancias de transacción (10 principales)	✓	✓
Topología de instancia de transacción	✓	✓
Topología de aplicación	✓	✓
Instrumentación automática de inyección JavaScript	N/A	✓

Reconfiguración de Supervisión de tiempo de respuesta en Windows

Utilice el mandato de configuración interactiva `rt-agent` o el programa de utilidad IBM Cloud Application Performance Management para configurar o volver a configurar el agente.

Antes de empezar

Si está habilitando la supervisión de transacciones HTTPS, asegúrese de que Monitoring Agent for HTTP Server no esté instalado en la misma máquina. De lo contrario, la configuración de Supervisión de tiempo de respuesta no cambiará el valor de HTTPS para el Analizador de paquetes.

Acerca de esta tarea

El agente de Supervisión de tiempo de respuesta se configura automáticamente a continuación de la instalación. Siga las instrucciones de instalación: “Planificación de la instalación ” en la página 712. Puede que sea necesario reconfigurarlo, por ejemplo, si desea supervisar un puerto diferente o transacciones HTTPS.

Se hace referencia al directorio de instalación como *dir_instalación*. El directorio de instalación predeterminado es: `C:\IBM\APM\`

Como alternativa a la utilización del mandato de configuración interactivo `rt-agent`, puede configurar el agente en el programa de utilidadIBM Cloud Application Performance Management. Para obtener más información, consulte “Utilización de la ventana de IBM Cloud Application Performance Management en sistemas Windows” en la página 189.

Procedimiento

Para personalizar los valores de datos, siga los pasos siguientes:

1. En el sistema en que se ha instalado el agente de Supervisión de tiempo de respuesta, detenga el agente:

   dir_instalación\BIN\rt-agent.bat stop
2. Utilice la configuración para configurar el agente:

   ```
   dir_instalación\BIN\rt-agent.bat config
   dir_instalación\samples\rt_silent_config.txt
   ```

   Para habilitar la supervisión de transacciones HTTPS, elimine el comentario de las líneas siguientes del archivo de configuración silenciosa. El archivo `rt_silent_config.txt` para configurar el agente de Supervisión de tiempo de respuesta para supervisar HTTPS en Windows debe ser similar al siguiente:

   ```
   # Monitor HTTPS transactions
   KT5MONITORHTTPSAPP=YES

   # HTTPS keystore (e.g. - /tmp/keys.kdb)
   KT5KEYSTORE=C:\keys\key.kdb

   # HTTPS server certificate map (eg - certAlias,9.48.152.1,443;...)
   KT5SERVERMAP=certalias,9.48.152.1,443
   # Monitor network traffic for the NIC hosts this IP address
   #KT5MONITORIP=9.48.152.1
   ```
3. Reinicie el agente de Supervisión de tiempo de respuesta para que los cambios entren en vigor:

   dir_instalación\BIN\rt-agent.bat start

Resultados

Los datos del origen nuevo se visualizan en los paneles de instrumentos asociados a Supervisión de tiempo de respuesta.

Reconfiguración de la Supervisión de tiempo de respuesta en AIX y Linux

Utilice el mandato de configuración `rt-agent` para configurar o reconfigurar el agente de Supervisión de tiempo de respuesta.

Acerca de esta tarea

El agente de Supervisión de tiempo de respuesta se configura automáticamente a continuación de la instalación. Siga las instrucciones de instalación: “Planificación de la instalación ” en la página 712. Puede que sea necesario reconfigurarlo, por ejemplo, si desea supervisar un puerto diferente.

El directorio de instalación se denomina *dir_instalación*. El directorio de instalación predeterminado es `/opt/ibm/apm/agent`.

Utilice el mismo usuario root que ha utilizado para instalar el agente para iniciar, detener y configurar el agente.

Procedimiento

Para reconfigurar, siga estos pasos:

1. En el sistema en que se ha instalado el agente de Supervisión de tiempo de respuesta, detenga el agente:

   ```
   dir_instalación/bin/rt-agent.sh stop
   ```
2. Utilice la configuración interactiva o silenciosa:

   a) Configuración interactiva:

   ```
   dir_instalación/bin/rt-agent.sh config
   ```

   b) Configuración silenciosa:

```
dir_instalación/bin/rt-agent.sh config  dir_instalación/samples/rt_silent_config.txt
```

Para habilitar la supervisión de transacciones HTTPS, elimine el comentario de las líneas siguientes del archivo de configuración silenciosa. El archivo `rt_silent_config.txt` para configurar el agente de Supervisión de tiempo de respuesta para supervisar HTTPS en AIX y Linux debe ser similar al siguiente:

```
# Monitor HTTPS transactions
KT5MONITORHTTPSAPP=YES

# HTTPS keystore (e.g. - /tmp/keys.kdb)
KT5KEYSTORE=/tmp/keys.kdb

# HTTPS server certificate map (eg - certAlias,9.48.152.1,443;...)
KT5SERVERMAP=certalias,9.48.152.1,443
# Monitor network traffic for the NIC hosts this IP address
#KT5MONITORIP=9.48.152.1
```

3. Reinicie el agente de Supervisión de tiempo de respuesta para que los cambios entren en vigor:
   `dir_instalación/bin/rt-agent.sh start`

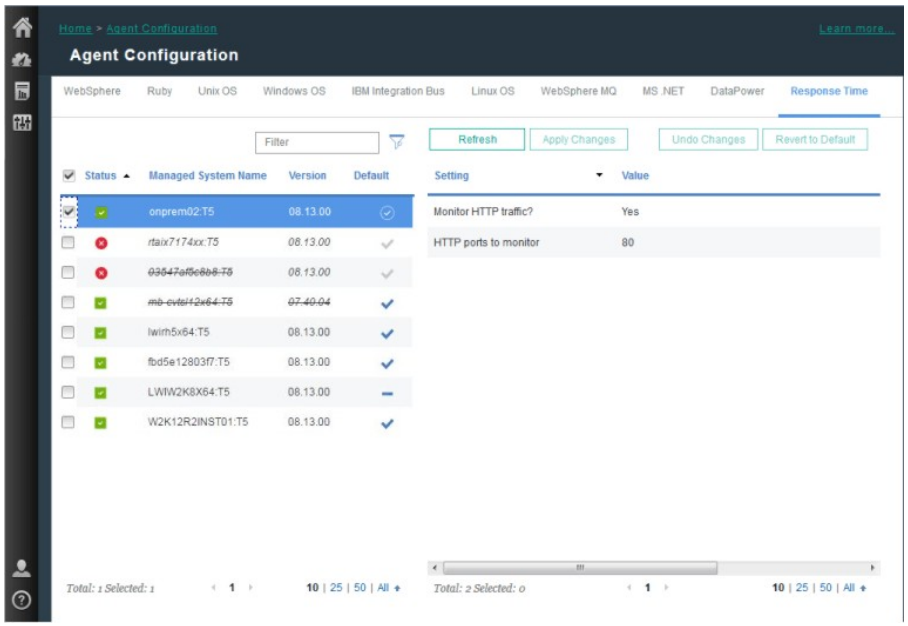
Resultados
Los datos del origen nuevo se visualizan en los paneles de instrumentos asociados a Supervisión de tiempo de respuesta.

Configuración de la página Configuración de agente

Puede utilizar la página **Configuración de agente** de la Consola de Cloud APM para ver qué agentes están instalados. Cuando sea aplicable, puede inhabilitar o habilitar la supervisión de transacciones HTTP y establecer los puertos supervisados por agentes Supervisión de tiempo de respuesta.

Configuración del agente

Para acceder a la página Supervisión de tiempo de respuesta **Configuración de agente**, en Consola de Cloud APM, seleccione **Configuración del sistema** > **Configuración de agente** y, a continuación, seleccione la pestaña **Tiempo de respuesta**.



La página **Configuración de agente** lista los sistemas del entorno en el que Supervisión de tiempo de respuesta está instalado.

Para cada sistema con un agente Supervisión de tiempo de respuesta instalado, la página **Configuración de agente** muestra:

- Si el sistema está en línea (marca de selección con fondo verde) o fuera de línea (cruz con fondo rojo).
- La versión del agente de Supervisión de tiempo de respuesta que está instalada.
- Si la configuración central no puede determinar el tipo del agente (es decir, si el Analizador de paquetes o Módulo de Tiempo de respuesta de IBM HTTP Server se utiliza para supervisar las transacciones HTTP), sólo está tachado el agente. Generalmente, el tipo de agente no se puede determinar cuando el agente no envía detalles de agente a través de actividad de ASF.
- Si el sistema utiliza los valores de configuración por omisión o tiene establecidos algunos valores personalizados.
- Los puertos que son supervisados si el agente de Supervisión de tiempo de respuesta está utilizando el Analizador de paquetes para supervisar las transacciones HTTP.

Setting	Value
Monitor HTTP traffic?	Yes
HTTP ports to monitor	80

- Si Módulo de Tiempo de respuesta de IBM HTTP Server, junto con Agente de HTTP Server, se utiliza para supervisar transacciones HTTP.

Setting	Value
Is IBM HTTP Server Response Time module enabled?	Yes

Consejo: Módulo de Tiempo de respuesta de IBM HTTP Server supervisa transacciones HTTP y HTTPS automáticamente. No es necesaria ninguna configuración del agente Supervisión de tiempo de respuesta.

Seleccione un agente para visualizar sus valores de configuración. Para encontrar un agente específico, escriba parte o todo el nombre del sistema en el que está instalado en el campo **Filtro**.

Las personalizaciones efectuadas en la página **Configuración de agente** tienen prioridad sobre cualquier otra personalización y sobre los valores predeterminados.

Si cambia de opinión acerca de los valores modificados, pulse **Deshacer cambios** para revertir a los últimos valores guardados, o pulse **Revertir a predeterminado** para volver a los valores predeterminados.

Los valores de configuración nuevos se envían a los Servicios de configuración central y los agentes en línea se reconfiguran automáticamente sin necesidad de reiniciarlos. Si el agente está fuera de línea, descarga los valores de configuración nuevos cuando pasa a estar en línea. Los datos de los puertos nuevos se visualizan en los paneles de instrumentos asociados con Supervisión de tiempo de respuesta cuando se renuevan los datos.

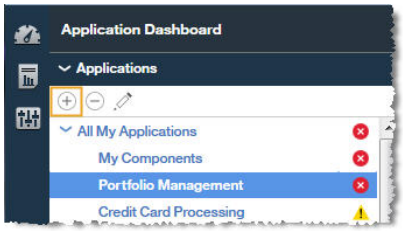
Adición de aplicaciones

Después de instalar el agente de Supervisión de tiempo de respuesta, puede que sea necesario añadir las aplicaciones que desea supervisar al Application Performance Dashboard.

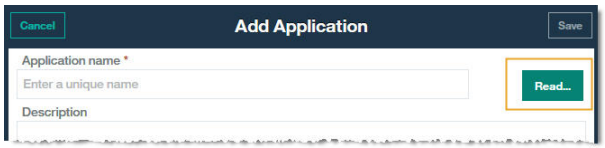
Procedimiento

Para añadir aplicaciones al Application Performance Dashboard:

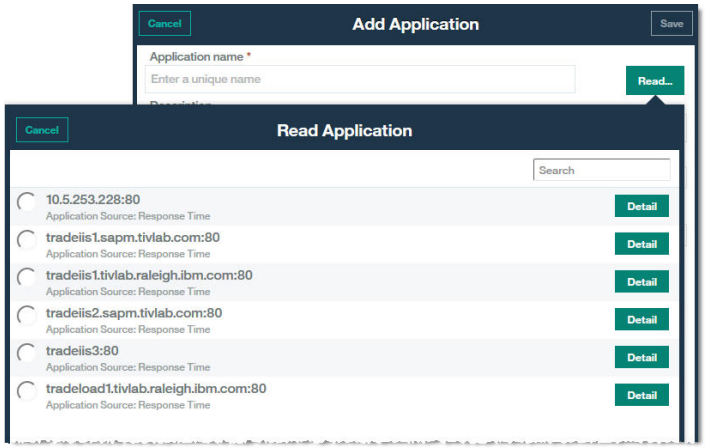
1. En Application Performance Dashboard, pulse **Añadir aplicación**.



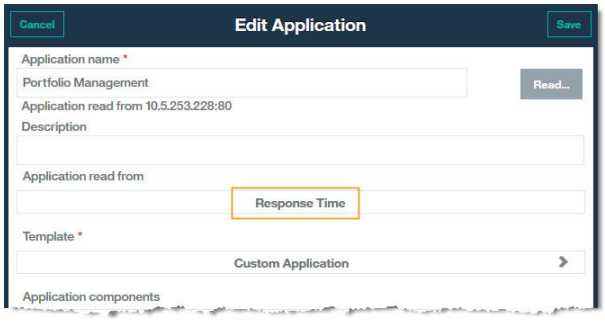
2. Seleccione **Lectura** para abrir una lista de aplicaciones descubiertas.



3. Seleccione la aplicación que desea supervisar.



Tiempo de respuesta se visualiza como repositorio de origen en el campo **Aplicaciones leídas desde:** y los componentes se listan en **Componentes de la aplicación**.



4. No es necesaria más configuración para visualizar las aplicaciones supervisadas por el agente Supervisión de tiempo de respuesta en Application Performance Dashboard. Pulse **Guardar** en la ventana **Añadir aplicación**.

Resultados

Las aplicaciones detectadas por el agente Supervisión de tiempo de respuesta se listan en **Todas mis aplicaciones** en Application Performance Dashboard.

Configuración del Módulo de Tiempo de respuesta de IBM HTTP Server

Para IBM HTTP Server y Apache HTTP Server, utilice el Módulo de Tiempo de respuesta de IBM HTTP Server para ver métricas de supervisión de tiempo de respuesta real del usuario final para páginas HTTP.

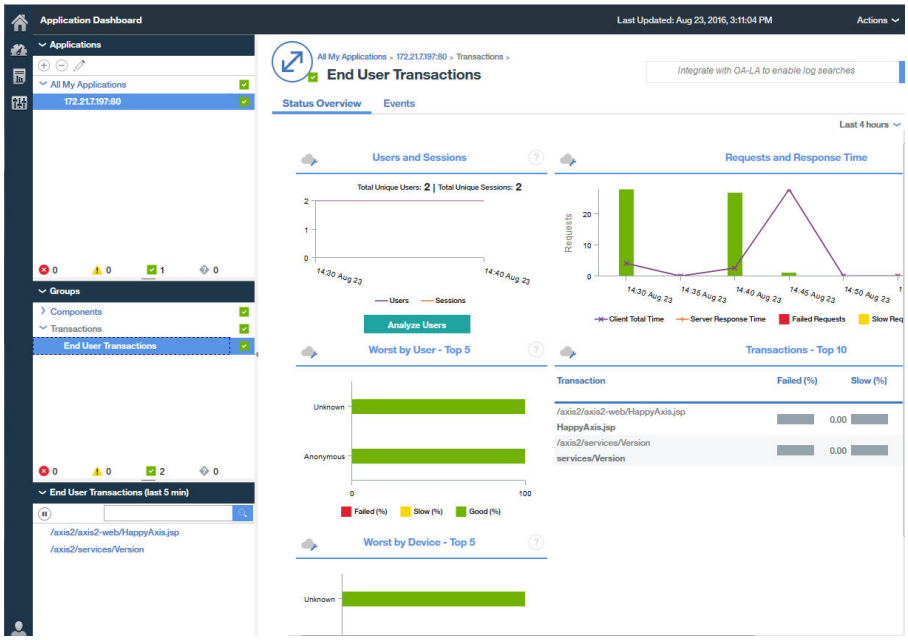
El Módulo de Tiempo de respuesta de IBM HTTP Server se instala y configura como parte del Agente de HTTP Server. El Módulo de Tiempo de respuesta de IBM HTTP Server sólo funciona junto con IBM HTTP

Server y Apache HTTP Server en AIX, Linux y Windows. El Módulo de Tiempo de respuesta de IBM HTTP Server supervisa todos los puertos para detectar solicitudes HTTP y HTTPS.

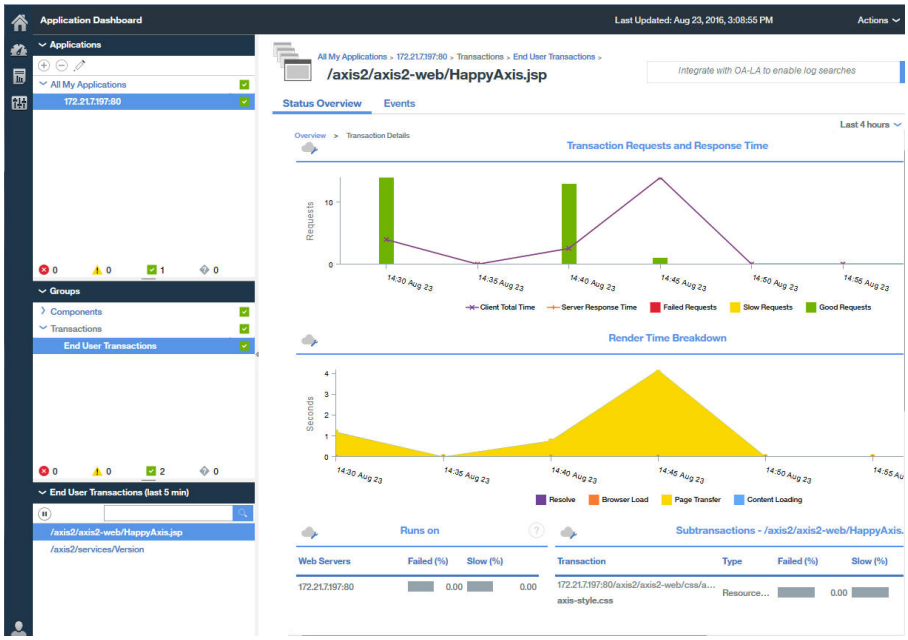
Mediante JavaScript, el Módulo de Tiempo de respuesta de IBM HTTP Server inserta una cabecera en las páginas web servidas por IBM HTTP Server para que el agente de Supervisión de tiempo de respuesta pueda supervisar esas páginas. Mediante cookies se realiza un seguimiento de los objetos incluidos cargados por la página. A continuación, la información de transacción de las páginas web servidas por IBM HTTP Server o Apache se incluye en los paneles de instrumentos de Transacciones de usuario final.

Por ejemplo:

Espacio de trabajo de Transacciones de usuario final que muestra datos recopilados del Módulo de Tiempo de respuesta de IBM HTTP Server en las Transacciones - 10 principales:



Espacio de trabajo de Transacciones de usuario final que muestra datos recopilados desde el Módulo de Tiempo de respuesta de IBM HTTP Server en la tabla **Subtransacciones** table



Módulo de Tiempo de respuesta de IBM HTTP Server

El Módulo de Tiempo de respuesta de IBM HTTP Server forma parte del Agente de HTTP Server. Sin embargo, funciona junto con el agente de Supervisión de tiempo de respuesta para supervisar transacciones de aplicación en servidores HTTP soportados.

Si instala el agente de Supervisión de tiempo de respuesta para que funcione con el Módulo de Tiempo de respuesta de IBM HTTP Server, se supervisarán todos los puertos para solicitudes HTTP y HTTPS.

El Módulo de Tiempo de respuesta de IBM HTTP Server forma parte del Agente de HTTP Server. Debe instalar el Agente de HTTP Server antes que el agente de Supervisión de tiempo de respuesta o instalarlo simultáneamente.

El Agente de HTTP Server se compone de dos plug-ins:

1. `khu_module` - este es el Agente de HTTP Server. Este plug-in es responsable de todos los paneles de instrumentos asociados con el Agente de HTTP Server. Para obtener más información, consulte la Referencia de Agente de HTTP Server.
2. `wrt_module` - este es el Módulo de Tiempo de respuesta de IBM HTTP Server.

Estos dos plug-ins están indicados en el archivo de configuración del Agente de HTTP Server. El archivo de configuración del Agente de HTTP Server es el siguiente para Apache HTTP Server:

```
khu.usr.local.apache24.conf.httpd.conf
```

El archivo es el siguiente para IBM HTTP Server:

```
khu.opt.IBM.HTTPServer.conf.httpd.conf
```

La regla de denominación de este archivo es: `khu.(vía de acceso completa del archivo de configuración del servidor http, cambie / por .).conf`

```
LoadModule khu_module

LoadModule wrt_module
```

Para que el Módulo de Tiempo de respuesta de IBM HTTP Server funcione, el archivo de configuración del servidor HTTP debe contener una sentencia include que haga referencia al archivo de configuración del Agente de HTTP Server. Por ejemplo:

```
include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
```

Esta sentencia include habilita ambos plugins simultáneamente. Para obtener más información, consulte “Configuración de la supervisión de HTTP Server” en la página 278.

Instalación y configuración del Módulo de Tiempo de respuesta de IBM HTTP Server

La configuración es automática en el lado del agente de Supervisión de tiempo de respuesta. El Módulo de Tiempo de respuesta de IBM HTTP Server debe instalarse y configurarse como parte del Agente de HTTP Server. El agente de Supervisión de tiempo de respuesta detecta automáticamente el Módulo de Tiempo de respuesta de IBM HTTP Server y lo habilita.

Acerca de esta tarea

Procedimiento

1. Instale el Agente de HTTP Server, que instala automáticamente el Módulo de Tiempo de respuesta de IBM HTTP Server.
2. Configure el Agente de HTTP Server. Esto habilitará el Módulo de Tiempo de respuesta de IBM HTTP Server. Para obtener más información, consulte “Configuración de la supervisión de HTTP Server” en la página 278.

3. Instale el agente de Agente de Supervisión de tiempo de respuesta como `root` o `Administrator`, dependiendo del sistema operativo. Para obtener instrucciones detalladas, consulte Capítulo 6, “Instalación de los agentes”, en la página 125.
4. Reinicie el IBM HTTP Server. Cuando el instalador de Supervisión de tiempo de respuesta detecte el Agente de HTTP Server, el agente de Supervisión de tiempo de respuesta habilitará el Módulo de Tiempo de respuesta de IBM HTTP Server automáticamente.

Habilitación manual de Módulo de Tiempo de respuesta de IBM HTTP Server

Para habilitar el manualmente Módulo de Tiempo de respuesta de IBM HTTP Server para supervisar el rendimiento de páginas HTTP y objetos incluidos para páginas web servidas por IBM HTTP Server.

Acerca de esta tarea

El Módulo de Tiempo de respuesta de IBM HTTP Server se habilita automáticamente cuando se instala y configura el Agente de HTTP Server. Sin embargo, es posible que desee habilitar manualmente el Módulo de Tiempo de respuesta de IBM HTTP Server.

Procedimiento

Para habilitar manualmente Módulo de Tiempo de respuesta de IBM HTTP Server en Linux, AIX o Windows, siga estos pasos:

1. Linux AIX
   Para habilitar manualmente el Módulo de Tiempo de respuesta de IBM HTTP Server en Linux o AIX, siga estos pasos:
   a) Detenga el agente Supervisión de tiempo de respuesta.
      Ejecutar
      ```
      $AGENT_HOME/bin/rt-agent.sh stop
      ```
      donde *$AGENT_HOME* puede ser `/opt/ibm/apm/agent` en un sistema Linux o `/opt/ibm/ccm/agent` en un sistema AIX.
   b) Ejecute un mandato de configuración y utilice *$AGENT_HOME*`/samples/rt_silent_config_ihs.txt` para añadir los módulos de carga en el archivo de configuración del servidor web y establecer los parámetros de configuración para el Módulo de Tiempo de respuesta de IBM HTTP Server.
   c) Reinicie el agente Supervisión de tiempo de respuesta.
2. Windows
   Para habilitar manualmente Módulo de Tiempo de respuesta de IBM HTTP Server en Windows, siga estos pasos:
   a) Detenga el agente Supervisión de tiempo de respuesta.
      Ejecutar
      ```
      AGENT_HOME/bin/rt-agent.bat stop
      ```
      donde *AGENT_HOME* puede ser `C:\IBM\APM` en un sistema Windows.
   b) Ejecute un mandato de configuración y utilice *AGENT_HOME*`\samples\rt_silent_config_ihs.txt` para añadir los módulos de carga en el archivo de configuración del servidor web y establecer los parámetros de configuración para el Módulo de Tiempo de respuesta de IBM HTTP Server.
      Por ejemplo,
      ```
      AGENT_HOME\bin\rt_agent.bat config AGENT_HOME\samples\rt_silent_config_ihs.txt
      ```
   c) Reinicie el agente Supervisión de tiempo de respuesta.

Inhabilitación manual de Módulo de Tiempo de respuesta de IBM HTTP Server

Para inhabilitar el Módulo de Tiempo de respuesta de IBM HTTP Server y volver a utilizar el analizador de paquetes, vuelva a configurar el agente y desactive la supervisión del Módulo de Tiempo de respuesta de IBM HTTP Server.

Acerca de esta tarea

Use los procedimientos siguientes para inhabilitar Módulo de Tiempo de respuesta de IBM HTTP Server.

Procedimiento

Para volver a configurar el agente interactivamente en Linux, AIX o Windows, siga estos pasos:

1. Linux AIX

   Para volver a configurar el agente interactivamente en Linux y AIX, siga estos pasos:

   a) Ejecute *dir_instalación*/bin/rt-agent.sh config
   Donde *dir_instalación* es /opt/ibm/apm/agent en Linux y AIX.

   b) Reinicie el agente Supervisión de tiempo de respuesta.

   De forma alternativa, para establecer los parámetros manualmente:

   a) Abra *dir_instalación*/config/*nombre_host*_t5.cfg en un editor de texto.
   donde *dir_instalación* es /opt/ibm/apm/agent en Linux y AIX.

   b) Establezca los parámetros siguientes:

   ```
   KT5DISABLEANALYZER=NO
   KT5ENABLEWEBPLUGIN=NO
   ```

   c) Reinicie el agente Supervisión de tiempo de respuesta.

2. Windows

   Para volver a configurar el agente interactivamente en Windows, siga estos pasos:

   a) Establezca manualmente los parámetros relacionados, abra *dir_instalación*\TMAITM6_x64*nombre_host*_t5.cfg en un editor de texto.
   donde *dir_instalación* es C:\IBM\APM en Windows.

   b) Establezca los parámetros siguientes:

   ```
   KT5DISABLEANALYZER=NO
   KT5ENABLEWEBPLUGIN=NO
   ```

   c) Reinicie el agente Supervisión de tiempo de respuesta.

Configuración avanzada de Módulo de Tiempo de respuesta de IBM HTTP Server

Existen diversas opciones de configuración avanzada para el Módulo de Tiempo de respuesta de IBM HTTP Server.

El Módulo de Tiempo de respuesta de IBM HTTP Server se configura automáticamente, pero hay una serie de tareas de configuración avanzada que puede realizar para ajustar el rendimiento y las características.

Inhabilitación de la supervisión de temporización de recursos

La supervisión de temporización de recursos está habilitada para todas las instancias de Módulo de Tiempo de respuesta de IBM HTTP Server instaladas mediante Agente de HTTP Server.

Acerca de esta tarea

Si desea reducir el número de recursos supervisados por Módulo de Tiempo de respuesta de IBM HTTP Server, o inhabilitar la supervisión de temporización de recursos para reducir la carga de proceso necesaria para supervisar un IBM HTTP Server concreto, complete los siguientes pasos:

Procedimiento

Para editar el archivo de configuración de Agente de HTTP Server generado, siga estos pasos:

1. Al final del archivo de configuración del servidor HTTP (httpd.conf), añada

```
WrtMaxPostResourcesSize
```

2. Establezca uno de los siguientes valores:
   - `WrtMaxPostResourcesSize -1`, para supervisar todos los recursos
   - `WrtMaxPostResourcesSize 0`, para desactivar la supervisión de recursos
   - `WrtMaxPostResourcesSize` *n*, par supervisar un determinado número de recursos, `10` de forma predeterminada. Por ejemplo, establezca `WrtMaxPostResourcesSize 2` para establecer un máximo de dos recursos para publicarlos en el servidor.
3. Reinicie el servidor HTTP.

Inhabilitación de la generación de ARM Correlator

De forma predeterminada, la generación del correlacionador ARM está habilitada lo que permite al Módulo de Tiempo de respuesta de IBM HTTP Server enlazarse a cualquiera de los servidores de fondo de la topología. Si es necesario, puede inhabilitar la generación de ARM Correlator.

Acerca de esta tarea

Restricción: Si inhabilita la generación del correlacionador ARM, Módulo de Tiempo de respuesta de IBM HTTP Server no podrá enlazarse a servidores de fondo como, por ejemplo, WebSphere Application Server. Inhabilite la generación de ARM Correlator solo si así se lo indica el personal de soporte de software de IBM.

Procedimiento

Para inhabilitar la generación de ARM Correlator, realice los pasos siguientes:

1. Al final del archivo de configuración del servidor HTTP (httpd.conf), añada

```
WrtDisableArmCorr
```

2. Reinicie el servidor HTTP

Inhabilitación de Supervisión de tiempo de respuesta con Tiempo de cliente (instrumentación JavaScript)

En IBM Application Performance Management, Supervisión de tiempo de respuesta con Tiempo de cliente (instrumentación JavaScript) está habilitado para todas las instalaciones de IBM HTTP Server que se ejecutan en todos los sistemas.

Acerca de esta tarea

Procedimiento

Para inhabilitar la inyección de JavaScript manualmente, realice los pasos siguientes:

1. Abra el archivo de configuración del servidor HTTP ubicado en: *raíz_HTTP_Server*`/conf/httpd.conf`
2. Desplácese hasta la línea añadida para el agente de HTTP Server y añada la línea siguiente después de ella:

```
WrtDisableJSI
```

   Por ejemplo,

```
include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.confWrtDisableJSI
```

3. Guarde el archivo `httpd.conf` y reinicie el servidor HTTP.

Eludir la cookie WRTCorrelator

Cuando la inyección JavaScript está habilitada para el agente Supervisión de tiempo de respuesta en WebSphere Portal, es posible que cookies como por ejemplo WRTCorrelator causen problemas al utilizar WebSphere Portal. Para evitarlos, puede establecer la cookie WRTCorrelator en Ignore.

Procedimiento

1. Si es necesario, inicie el servidor `WebSphere_Portal`.
2. Inicie sesión en WebSphere® Integrated Solutions Console.
3. Vaya a **Recursos** > **Entorno de recursos** > **Proveedores de entorno de recursos**.
4. Seleccione **WP ConfigService**.
5. En Propiedades adicionales, seleccione **Propiedades personalizadas**.
6. Pulse **Nuevo**.
7. Especifique el nombre de la propiedad, la cookie WRTCorrelator en este caso, y establezca el valor de la propiedad en Ignore.

   Para establecer la cookie WRTCorrelator en Ignore, especifique lo siguiente:

   ```
   cookie.ignore.regex =
   digest\.ignore.*|LTPAToken|LTPAToken2|JSESSIONID|WASReqURL|WRTCorrelator
   |PD_STATEFUL.*
   ```

8. Pulse **Aplicar** y guarde los cambios.
9. Cierre la sesión de WebSphere® Integrated Solutions Console.

Resultados

La cookie WRTCorrelator se establece en Ignore y se evitan problemas como por ejemplo bucles.

Exclusión de páginas de informes de tiempo del cliente

Quizá quiera excluir del navegador ciertas páginas de los informes de tiempo del cliente.

Acerca de esta tarea

Puede añadir un parámetro al archivo de configuración para detener el Módulo de Tiempo de respuesta de IBM HTTP Server y que no inyecte JavaScript en ningún archivo que coincida con los patrones que especifique. Esto, a su vez, detiene los informes de tiempo de cliente del navegador para esas páginas.

Procedimiento

Para excluir del navegador ciertas páginas de los informes de tiempo del cliente, complete los pasos siguientes:

1. Abra el siguiente archivo en un editor de texto:

   Linux AIX *dir_instalación*`/config/`*nombrehost*`_t5.cfg`, donde *dir_instalación* es `/opt/ibm/apm/agent`

   Windows *dir_instalación*`\TMAITM6_x64\`*nombre_host*`_t5.cfg` donde *dir_instalación* es `C:\IBM\APM`

2. En la sección **advconfig**, añada

   ```
   {KT5WEBPLUGIN_JSI_EXCLUDE_URI_WITH_PATTERNS=patrón_vía_URL_a_excluir}
   ```

   Por ejemplo,

   ```
   {KT5WEBPLUGIN_JSI_EXCLUDE_URI_WITH_PATTERNS=*/DoNotJSIMe.jsp,/absolutePath/index.jsp,/
   skipThisDir/*}
   ```

   La vía de acceso de URL tiene una limitación de 256 caracteres.

Consejo: Utilice un asterisco (*) como prefijo o sufijo para la coincidencia de patrones. Si es necesario, añada varios valores separados por una coma al parámetro.

3. Guarde y cierre *nombre_host*_t5.cfg.
4. Reinicie el agente Supervisión de tiempo de respuesta:

```
rt-agent.sh stop
rt-agent.sh start
```

Utilización de Módulo de Tiempo de respuesta de IBM HTTP Server como usuario no root

Con cierta configuración detallada, puede utilizar el Módulo de Tiempo de respuesta de IBM HTTP Server con un ID de usuario distinto de `root`. Recuerde que si utiliza el Analizador de paquetes de red, debe utilizar el usuario `root`.

Para utilizar un ID de usuario distinto de `root`, siga estas directrices.

Para el agente de Supervisión de tiempo de respuesta

Instale el agente de Supervisión de tiempo de respuesta mediante el ID de usuario con el que lo va a ejecutar, en un directorio que tenga acceso de escritura.

- Para este procedimiento, el ID de usuario del agente de Supervisión de tiempo de respuesta es *agentuser*. El directorio en el que se instala el agente es *$AGENT_HOME*.
- Si instala el agente de Supervisión de tiempo de respuesta como `root` y, a continuación, ejecuta el agente como un usuario distinto, no podrá crear archivos.

Para Módulo de Tiempo de respuesta de IBM HTTP Server

`ServerRoot` debe ser propiedad del mismo ID de usuario que se utiliza para ejecutar `apache start|stop`.

- Durante la acción `apache start`, se crea un directorio de seguimiento `wrt` en `ServerRoot`. Por lo tanto, el usuario necesita suficientes permisos para crear archivos y directorios en `ServerRoot`.
- Si el usuario del Módulo de Tiempo de respuesta de IBM HTTP Server, *ihsuser* es diferente de *agentuser*, se requiere acceso de grabación en `$AGENT_HOME/tmp`.

  Se crea `$AGENT_HOME/tmp` durante la instalación de los agentes. *ihsuser* necesita permiso para crear un directorio `kt5` en `$AGENT_HOME/tmp`.
- Puede haber varias versiones de `ServerRoot`, cada una de ellas administrada por usuarios distintos.

Para el agente de Supervisión de tiempo de respuesta y Módulo de Tiempo de respuesta de IBM HTTP Server

Tanto *agentuser* como *ihsuser* necesitan acceso de lectura y escritura en los directorios siguientes:

- `$AGENT_HOME/tmp/kt5`
- `ServerRoot/wrt`

Normalmente, el Módulo de Tiempo de respuesta de IBM HTTP Server se inicia en primer lugar y los directorios `wrt` los crea automáticamente Supervisión de tiempo de respuesta cuando se inicia por primera vez, con acceso de lectura/escritura para todos.

`ServerRoot/wrt` también lo utiliza `camconfig` para iniciar la configuración. El usuario *ihsuser* crea archivos de ID de cola compartida que los recoge el usuario *agentuser*; *agentuser* lee el ID de cola del directorio e inicia la configuración.

Si se utiliza `root` para ejecutar `apache start` inicialmente y el usuario *ihsuser* no es `root`, lleve a cabo los pasos siguientes:

1. Detenga el agente Supervisión de tiempo de respuesta.
2. Utilizando `root`, ejecute `apachectl stop`.
3. Suprima los siguientes directorios:

- $AGENT_HOME/tmp/kt5
- ServerRoot/wrt

4. Utilizando *ihsuser*, ejecute `apachectl start` para volver a crear los directorios con los permisos correctos.

Para restablecer el permiso del Módulo de Tiempo de respuesta de IBM HTTP Server al directorio `wrt`

Para mayor seguridad, puede restablecer el permiso del directorio `wrt` del Módulo de Tiempo de respuesta de IBM HTTP Server. La actualización implica añadir un parámetro en el archivo de configuración para limitar el permiso al directorio `wrt` que ha creado el usuario no root durante la instalación de IBM HTTP Server.

Complete el procedimiento en el sistema donde está instalado el Módulo de Tiempo de respuesta de IBM HTTP Server para cambiar el permiso del directorio `wrt` para el usuario no root de 777 a 700:

1. Abra el archivo IHS_HOME/conf/httpd.conf en un editor de texto.
2. Añada la propiedad **WrtDisableDirPermNonRoot** al final del archivo:
   - Cuando la propiedad está habilitada, sólo se utiliza para crear el directorio `wrt` con permiso 700 el ID de usuario que ha iniciado httpd y que coincide con el ID de usuario que ha creado el directorio. Se deniega el acceso para trabajar con este directorio a todos los demás usuarios.
   - Cuando la propiedad no está habilitada, se crea el directorio `wrt` con el permiso predeterminado 777.
3. Reinicie el agente Supervisión de tiempo de respuesta:

```
rt-agent.sh stop
rt-agent.sh.start
```

Los datos de configuración de Supervisión de tiempo de respuesta y algunos archivos persistentes se almacenan en el directorio `wrt`, que se utiliza durante el proceso de comunicación, y cada proceso de conexión crea un archivo de configuración wrt en el directorio. Tras añadir **WrtDisableDirPermNonRoot** al archivo `httpd.conf`, sólo el usuario determinado limitado puede comunicarse con éxito con el agente de supervisión de Supervisión de tiempo de respuesta.

Utilización de equilibradores de carga
Si utiliza equilibradores de carga en el entorno, deberá realizar algunos ajustes adicionales.

Procedimiento

Si está utilizando un equilibrador de carga, siga estas directrices:

1. Desactive la Reescritura de URL en el equilibrador de carga.
2. Instale un agente de Supervisión de tiempo de respuesta en cada servidor web que desee supervisar.

   No instale Supervisión de tiempo de respuesta en el equilibrador de carga.

Qué hacer a continuación

Si está ejecutando el agente Supervisión de tiempo de respuesta tras un equilibrador de carga, puede configurar el equilibrador de carga para reenviar la dirección IP del cliente para optimizar el rendimiento de supervisión. Siga estos pasos como ejemplo:

1. En la cabecera HTTP, establezca la dirección IP del cliente en el campo **X-Forwarded-For**.
2. En el archivo $AGENT_HOME/config/*nombre_host*_t5.cfg, añada {KT5WEBPLUGIN_OVERRIDE_SOURCE_ADDR_HEADERS=X-Forwarded-For} en la sección SECTION=advconfig.

   Consejo: Si es necesario, añada varios valores al parámetro. Por ejemplo, {KT5WEBPLUGIN_OVERRIDE_SOURCE_ADDR_HEADERS=x-forwarded-for, iv-remote-address}

3. Reinicie el agente Supervisión de tiempo de respuesta. Ejecute los mandatos siguientes:

```
rt-agent.sh stop
rt-agent.sh start
```

Limitar la CPU utilizada para supervisarIBM HTTP Server

En entornos saturados, es posible que desee limitar el porcentaje de CPU utilizada por la instrumentación de IBM HTTP Server.

Acerca de esta tarea

Especifique el porcentaje de CPU que puede utilizar Módulo de Tiempo de respuesta de IBM HTTP Server. De forma predeterminada el porcentaje de CPU no está limitado. Configure el porcentaje de CPU en el servidor donde está instalado el agente.

Procedimiento

Para configurar el porcentaje de CPU utilizada, realice los pasos siguientes:

1. Vuelva a configurar el agente de forma interactiva o manual:
   - Ejecute el script de agente para la configuración de forma interactiva:

     Linux AIX

     ```
     $AGENT_HOME/bin/rt-agent.sh config
     ```

     Windows

     ```
     dir_instalación\BIN\rt-agent.bat config
     ```

   - Abra el siguiente archivo en un editor de texto:

     Linux AIX

     ```
     /opt/ibm/apm/agent/config/nombre_host_t5.cfg
     ```

     Windows

     ```
     C:\IBM\APM\TMAITM6_x64\nombre_host_T5.cfg
     ```

2. En la sección **advconfig**, añada el siguiente parámetro y establezca un valor de 0 a 100:

   ```
   KT5WEBPLUGIN_TARGET_CPU_PERCENTAGE=10
   ```

   donde el valor que especifica es el límite de porcentaje del uso de CPU. El valor predeterminado de *0* significa que el uso de CPU no está limitado.
3. También puede establecer los siguientes parámetros:

Opción	Descripción
KT5WEBPLUGINCONFIGPOSTURL	Lista de URL correspondientes a una instalación de IBM HTTP Server. Valor predeterminado: `http://localhost/WrtUpdateConfig.dat`
KT5WEBPLUGIN_MAX_REQUESTS_PER_SECOND	Número de solicitudes por segundo supervisadas por cada instalación de IBM HTTP Server. Si el número de solicitudes sobrepasa este número, las solicitudes subsiguientes no se supervisarán. Si se llega al límite, la inserción JavaScript se detiene y

Opción	Descripción
	no se devuelve ningún datos al agente Supervisión de tiempo de respuesta. Valor predeterminado: 0 (sin máximo)
KT5WEBPLUGIN_CPUMAN_PERIOD_IN_SEC	Período, en segundos, en el que se comprueba el uso de CPU para determinar si se ha sobrepasado el objetivo. Valor predeterminado: 60 segundos
KT5WEBPLUGIN_CATCHUP_PERIOD_COUNT	Número de períodos permitidos en el mismo estado antes de que se escale la CPU hacia abajo. Por ejemplo, utilizando el valor predeterminado, si el uso de CPU es alto y 4 ciclos más tarde sigue siendo alto, el uso de CPU se escalará hacia abajo. Valor predeterminado: 3

Resultados
El porcentaje de CPU disponible en Módulo de Tiempo de respuesta de IBM HTTP Server se establece en un porcentaje fijo.

Hoja de ruta del Analizador de paquetes

Utilice el Analizador de paquetes para supervisar las transacciones HTTP. Es necesario configurar manualmente la supervisión de HTTPS. Será necesario instrumentar manualmente las páginas web para recopilar temporizadores de navegador.

Para determinar los entornos en los que puede utilizar el Analizador de paquetes, consulte “Supervisión de tiempo de respuestaComponentes” en la página 711 y “Planificación de la instalación ” en la página 712.

El Analizador de paquetes se habilita automáticamente cuando se instala el agente de Supervisión de tiempo de respuesta, pero hay diversos pasos y personalizaciones adicionales que puede que necesite realizar.

1. Puede personalizar los valores del Analizador de paquetes, por ejemplo, el número de puerto, en la ventana de Configuración de agente. Para obtener más información, consulte “Configuración del Analizador de paquetes utilizando la ventana Configuración de agente” en la página 729.
2. Para supervisar transacciones HTTPS, instrumente manualmente las páginas web para recopilar temporizadores de navegador. Para obtener más información, consulte “Supervisión de transacciones HTTPS” en la página 732.
3. Para habilitar las temporizaciones del navegador, añada el componente Inyección de JavaScript a la aplicación y asocie el componente de supervisión de JavaScript con la aplicación; para obtener más información, consulte “Adición del componente de supervisión de JavaScript a la aplicación” en la página 730.
4. Si está operando en un entorno de carga de transacciones elevada, puede que sea necesario realizar algunas tareas de ajuste avanzadas. Para obtener más información, consulte “Configuración avanzada del Analizador de paquetes” en la página 736

Configuración del Analizador de paquetes utilizando la ventana Configuración de agente
Puede utilizar la ventana Configuración de agente para configurar el Analizador de paquetes.

Para supervisar el tráfico HTTP para un sistema determinado utilizando el Analizador de paquetes, realice los pasos siguientes:

1. Para acceder al agente Configuración de agente, en Interfaz de usuario de APM, seleccione **Configuración del sistema** > **Configuración de agente** y, a continuación, seleccione la pestaña **Tiempo de respuesta**.
2. Seleccione el sistema o sistemas que desea actualizar. Seleccione varios sistemas si desea utilizar los mismos valores HTTP para cada uno de esos sistemas.

   Si los sistemas que selecciona tienen establecidos diferentes valores HTTP, se visualiza `Varios valores` o `Múltiples listas` en lugar de valores individuales. No se pueden actualizar los sistemas con valores diferentes al mismo tiempo.
3. En el campo **¿Supervisar tráfico HTTP?**, haga doble clic en el valor y seleccione **Sí** en la lista.
4. En el campo **Puertos HTTP a supervisar**, haga doble clic en el valor y especifique los puertos adicionales que desea supervisar, que no sean el puerto predeterminado 80 y los otros puertos ya listados.

   Para detener la supervisión de un puerto, seleccione el puerto que ya no desee supervisar y pulse **Eliminar**.
5. Pulse **Aplicar cambios**.

Adición del componente de supervisión de JavaScript a la aplicación

Para ayudarle a comprender el rendimiento de las páginas web en un navegador y los errores, es preciso que el agente de Supervisión de tiempo de respuesta pueda recopilar datos de temporización desde el navegador. Para habilitar esta característica, debe configurar la aplicación que desea supervisar.

Acerca de esta tarea

Para poder supervisar interacciones en sus páginas web, debe añadir el componente de supervisión de JavaScript a cada página web de la aplicación. El componente de supervisión de JavaScript captura el estado de cada páginas web y las interacciones de JavaScript asociadas. Añada el componente de supervisión de JavaScript a la aplicación que desee supervisar. El contenido y las acciones relevantes se capturan automáticamente y se envían al Servidor de Cloud APM para su análisis y correlación.

Procedimiento

Complete los pasos siguientes para habilitar la recopilación de datos reales de supervisión de usuario del navegador. Estos pasos solo se tienen que completar una vez, a menos que cambie la configuración de la aplicación.

1. Añada el componente de supervisión de JavaScript a la aplicación. El procedimiento que utilice dependerá del tipo de aplicación:
   a) Para las aplicaciones Java EE, extraiga *dir_instalación*`/clienttime/ClientTime.war` del paquete de instalación en un directorio accesible para HTTP Server.
   b) Para aplicaciones no Java EE como, por ejemplo, Ruby, .NET, Python y Node.js, guarde *dir_instalación*`/clienttime/wrtInstrumentation.js` del paquete de instalación en un directorio accesible para HTTP Server.

      Extraiga el archivo *dir_instalación*`/clienttime/ClientTime.war` en una vía de acceso temporal. Debe copiar el archivo `wrtTimingTarget.dat` extraído en el directorio raíz de documento. La raíz de documento es un valor de HTTP Server (Apache, IIS, etc.). Es un directorio para almacenar los documentos. De forma predeterminada, todas las solicitudes se toman de este directorio, pero pueden utilizarse enlaces simbólicos y alias para apuntar a otras ubicaciones. Por ejemplo, la raíz de documento para Apache es `/opt/IBM/HTTPServer/htdocs`.

      El archivo `wrtInstrumentation.js` se puede colocar en cualquier directorio. Asegúrese de actualizar la ubicación de vía de acceso al archivo `wrtInstrumentation.js` en la cabecera HTML.
2. Asocie el componente de supervisión de JavaScript a la aplicación.

Esta asociación se puede realizar normalmente modificando un script de cabecera de aplicación. Normalmente solo se debe modificar un script de cabecera para cada componente o aplicación que se supervise.

Tanto para aplicaciones Java EE como para aplicaciones no Java EE, añada el JavaScript siguiente a la cabecera de aplicación, delante de cualquier otro JavaScript:

```
<script language="JavaScript" src="vía_acceso/wrtInstrumentation.js"
type="text/JavaScript"></script>
```

donde *vía_acceso* es la vía de acceso relativa al componente de supervisión de JavaScript.

Por ejemplo:

```
<script language="JavaScript" src="/ClientTime/wrtInstrumentation.js"
type="text/JavaScript"></script>
```

Resultados

Se supervisan las páginas que se han instrumentalizado con el componente de supervisión JavaScript y los datos de las páginas se analizan y visualizan en paneles de instrumentos de Transacciones de usuario final.

Habilitación de la temporización en navegador

Mediante la habilitación de la supervisión por temporización de recursos, el agente de Supervisión de tiempo de respuesta procesa los datos de temporización de recursos W3C usando Analizador de paquetes. Con esta función habilitada, puede ver información de rendimiento detallada en elementos de componente frontal.

Acerca de esta tarea

Para poder supervisar datos de temporización de recursos, debe añadir el componente de supervisión de temporización de recursos a la aplicación y asociarlo con la aplicación. El componente de supervisión de temporización de recursos captura automáticamente el estado y las interacciones de los elementos de componente frontal y envía los datos al Servidor de Cloud APM para el análisis. Los resultados de este análisis se muestran en el panel de instrumentos **Subtransacciones**.

Procedimiento

Siga los pasos que se indican a continuación para habilitar la función de supervisión de temporización de recursos. Siga estos pasos una sola vez, a menos que cambie la configuración de la aplicación.

1. Añada el componente de supervisión de temporización de recursos a la aplicación.
   a) Extraiga el archivo *dir_instalación*/clienttime/wrtInstrumentation.js del paquete de instalación.
   b) Añada el archivo wrtInstrumentation.js al directorio JavaScript de la aplicación.
2. Añada la línea siguiente a la cabecera de aplicación:

```
<script> var wrt_enableResourceTiming=true; </script>
```

Por ejemplo,

```
<script language="JavaScript" src="vía_acceso/wrtInstrumentation.js"
type="text/JavaScript"></script>
<script> var wrt_enableResourceTiming=true; </script>
```

Resultados

Las páginas se instrumentan con el componente de supervisión de temporización de recursos. Este componente estará habilitado de forma predeterminada. Los datos de temporización de recursos de las

páginas instrumentadas con el componente de supervisión de temporización de recursos se analizan y visualizan en los paneles de instrumentos **Subtransacciones**.

Qué hacer a continuación

Si desea inhabilitar el componente de supervisión de temporización de recursos, establezca el parámetro **wrt_enableResourceTiming** en `false`.

Supervisión de transacciones HTTPS

Supervisión de tiempo de respuesta supervisa las transacciones HTTP de forma predeterminada. Para supervisar las transacciones HTTPS, Supervisión de tiempo de respuesta requiere acceder a los certificados SSL de modo que puede descifrar el tráfico SSL de los servidores web remotos.

Antes de empezar

Identifique los servidores web HTTPS que desea supervisar incluyendo las direcciones IP y los puertos configurados correspondientes. Por ejemplo, `192.168.1.23`, puerto 443. Para cada servidor web HTTPS, compruebe que Supervisión de tiempo de respuesta puede leer el cifrado. Supervisión de tiempo de respuesta soporta los cifrados soportados por IBM Java, lo que incluye los siguientes.

- RSA_WITH_RC4_40_MD5
- RSA_WITH_RC4_128_MD5
- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_40_SHA
- RSA_WITH_DES40_CBC_SHA
- RSA_WITH_DESC_CBC_SHA
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_256_CBC_SHA
- RSA_EXPORT1024_WITH_RC4_56_MD5
- RSA_EXPORT1024_WITH_RC2_CBC_56_MD5
- RSA_EXPORT1024_WITH_DES_CBC_SHA
- RSA_EXPORT1024_WITH_RC4_56_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Restricción: Supervisión de tiempo de respuesta no puede descifrar tráfico que utiliza el intercambio de claves Diffie-Hellman.

Procedimiento

Para habilitar la supervisión de transacciones HTTPS, siga estos pasos:

1. Configure el almacén de claves. Para obtener más información, consulte “Configuración del almacén de claves” en la página 733.
2. Configure el agente de Supervisión de tiempo de respuesta ejecutando uno de los mandatos siguientes y proporcionando los valores cuando se le solicite:

   Por ejemplo:

```
Configuración del agente de supervisión de tiempo de respuesta
¿Editar valores del 'Agente superv. tiempo respuesta'? [1=Sí,2=No] (valor predeterminado:
1): 1

Configuración básica :   Especifique la configuración de supervisión básica. Nota: Ahora
HTTP está
configurada de forma central utilizando la pestaña Tiempo de respuesta en Configuración de
agente.
```

```
Especifica si deben supervisarse las transacciones HTTPS
¿Desea supervisar las transacciones HTTPS? [ 1=Sí, 2=No ] (el valor predeterminado es:2): 1

Este almacén de claves contiene los certificados de los sitios web HTTPS que se están
supervisando
Almacén de claves HTTPS (por ejemplo, - /tmp/keys.kdb) (el valor predeterminado es: ): /tmp/
keys.kdb

Esta tabla correlaciona los servidores HTTPS con los certificados apropiados (por ejemplo,
cert1,
server ip,server port; cert2,server2 ip,server2 port);...
HTTPS server certificate map (eg - certAlias,9.48.152.1,443;...)(el valor predeterminado
es: ):
 label1,10.0.0.1,9443;label1,9.185.150.71,443

Configuración avanzada:
Especifique la configuración avanzada de supervisión

Se supervisará la tarjeta NIC que tiene la dirección IP seleccionada.
La dirección IP de la NIC que se va a supervisar (el valor predeterminado es: ): 10.0.0.1

Configuración de la recopilación de datos y análisis:
Especifique la información de configuración sobre cómo se analizan los datos.

La configuración se ha completado satisfactoriamente.
Es necesario reiniciar el agente para que se apliquen los cambios de configuración.
```

donde:

- El almacén de claves HTTPS es el almacén de claves configurado en el paso 1
- Correlación de certificados de servidor HTTPS, especifique:
  - `etiqueta 1` - la etiqueta clave configurada en el paso 1
  - `servidor ip` - la dirección IP del servidor, que debe coincidir con el atributo Origen/Destino en la cabecera IPV4 de los paquetes
  - `puerto de servidor` - número de puerto de servidor, que debe coincidir con el atributo de puerto de Origen/Destino en la cabecera TCP de los paquetes

  Añada varias entradas para varias posibilidades de la dirección IP del servidor de la misma etiqueta clave.
- La dirección IP de la tarjeta de interfaz de red que se va a supervisar, la interfaz que puede ver los paquetes y se correlaciona con eth0, en0, etc. El nombre no tiene que coincidir con ningún atributo de IPV4 ni las cabeceras TCP de los paquetes. Si `10.0.0.1` corresponde a eth0, utilice `tcpdump -s0 -i eth0 ...` para ver todos los paquetes que el Analizador de paquetes tiene que analizar.

3. Reinicie el agente Supervisión de tiempo de respuesta.

Configuración del almacén de claves

Para supervisar transacciones HTTPS, importe claves en KT5Keystore para todos los servidores web que desea supervisar.

Acerca de esta tarea

Puede exportar los certificados SSL desde los servidores web que está supervisando e impórtelos en el almacén de claves HTTP utilizando IBM Key Management (iKeyman), o especifique el archivo stash del almacén de claves del servidor web (`.kdb`) en el almacén de claves HTTPS. Cuando instala o configura Supervisión de tiempo de respuesta, se le solicita la ubicación del archivo `keys.kdb`.

Si no tiene archivos stash del almacén de claves (`.kdb` y `.sth`), compruebe que el proveedor CMS está habilitado en la versión de Java para poder utilizar iKeyman para configurar la base de datos de claves:

1. Vaya al directorio *dir_instalación*`/ibm-jre/jre/lib/security`. Por ejemplo:
   - Linux `/opt/ibm/apm/agent/JRE/lx8266/lib/security`
   - Windows `C:\Program Files\IBM\APM\ibm-jre\jre\lib\security`

2. En el archivo `java.security`, añada la sentencia siguiente a la lista de proveedores de seguridad como se muestra, donde *número* es la última secuencia de número de la lista.

   ```
   security.provider.número=com.ibm.security.cmskeystore.CMSProvider
   ```

   La lista de proveedores tiene un aspecto parecido al del ejemplo siguiente:

   ```
   ## Lista de proveedores y su orden de preferencia #
   security.provider.1=com.ibm.jsse.IBMJSSEProvider
   security.provider.2=com.ibm.crypto.provider.IBMJCE
   security.provider.3=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.4=com.ibm.security.cert.IBMCertPath
   security.provider.5=com.ibm.security.cmskeystore.CMSProvider
   ...
   #
   ```

3. Guarde los cambios y cierre el archivo.

Restricción: Supervisión de tiempo de respuesta no puede descifrar tráfico utilizando el intercambio de claves Diffie-Hellman.

Procedimiento

Para habilitar la supervisión de transacciones HTTPS, recopile los certificados SSL de los servidores web que desea supervisar e importe los certificados y los archivos de ocultación de almacén de claves en el almacén de claves HTTPS mediante iKeyman. En el ejemplo siguiente se utiliza iKeyman para exportar los certificados de un servidor IBM HTTP Server e importarlos en el almacén de claves HTTPS:

1. Instale un agente Supervisión de tiempo de respuesta en cada servidor web HTTPS que desea supervisar.
2. Ejecute **IBM Key Management** (iKeyman) desde el directorio `bin` de IBM Java ejecutando uno de los mandatos siguientes, en función del sistema operativo.
   - AIX Linux `/opt/ibm/apm/agent/JRE/lx8266/bin/ikeyman`

     Nota: Debe tener X-Window en el entorno para que iKeyman funcione adecuadamente.
   - Windows `c:\IBM\APM\java\java80_x64\jre\bin\ikeyman`
3. Cree una base de datos del almacén de claves nueva. En el cuadro de diálogo **Nuevo**, complete los pasos siguientes:
   a) Desde la lista **Tipo de base de datos de claves**, seleccione **CMS**.

      Si CMS no está disponible en la lista, es posible que el proveedor de CMS no esté habilitado. Habilite el proveedor de CMS en el archivo de seguridad de Java.

   b) En el campo **Nombre de archivo**, especifique el nombre del archivo del almacén de claves HTTPS y pulse **Aceptar**.
   Por ejemplo, `keys.kdb`.
4. En el cuadro de diálogo **Indicador de solicitud de contraseña**, complete los pasos siguientes:
   a) En los campos **Contraseña** y **Confirmar contraseña**, escriba y confirme la contraseña para acceder a `keys.kdb`.

      No establezca una hora de caducidad a menos que desee volver a crear la base de datos del almacén de claves y reiniciar el agente Supervisión de tiempo de respuesta periódicamente.

   b) Seleccione **¿Guardar la contraseña en un archivo stash?** para almacenar la contraseña de `keys.kdb` en un formato cifrado en un archivo stash, `keys.sth`.

      Nota: el agente de Tiempo de respuesta sólo da soporte a la versión 1 de contraseñas ocultas. A partir de APM 8.1.4, ejecute el mandato siguiente para almacenar la contraseña de keys.kdb en un archivo de ocultación cifrado, keys.sth.

      En Linux:

      ```
      cp keyfile.sth keyfile.sth.new-format
      ```

```
cd /opt/IBM/ccm/agent/lx8266/gs/bin
```

```
#export LD_LIBRARY_PATH=/opt/ibm/apm/agent/lx8266/gs/lib64:$LD_LIBRARY_PATH
```

```
./gsk8capicmd_64 -keydb -stashpw
-db /opt/IBM/ccm/agent/keyfiles/keyfile.kdb -v1stash
```

En Windows:

```
copy server.sth server.sth.backup
```

```
set PATH=c:\IBM\APM\GSK8_x64\lib64;%PATH%
```

```
C:\IBM\APM\GSK8_x64\bin\gsk8capicmd_64 -keydb
-stashpw -db .\server.kdb -pw passw0rd -v1stash
```

5. En la sección **Contenido de base de datos de claves** de la ventana iKeyman, realice los pasos siguientes:
   a) Seleccione **Certificados personales**.
   b) Pulse **Importar**.
   c) En el diálogo **Importar clave**, desde la lista **Tipo de archivo de claves**, seleccione **CMS**.
   d) Examine en busca del archivo del almacén de claves, pulse **Abrir**, y después pulse **Aceptar**.
   e) En el cuadro de diálogo **Indicador de solicitud de contraseña**, escriba la contraseña del almacén de datos.
   f) Seleccione la clave de la lista y pulse **Aceptar**.
   g) En el cuadro de diálogo **Cambiar etiquetas**, seleccione el nombre de etiqueta de la clave. En el campo **Especificar una etiqueta nueva**, indique el nombre de host del servidor y pulse **Aplicar**.

      Nota: Necesitará este valor cuando configure Supervisión de tiempo de respuesta, de modo que tome nota de él.
   h) Pulse **Aceptar**.
6. Guarde el almacén de claves HTTPS.

Importación de claves de Internet Information Services

Para extraer claves de Internet Information Services e importarlas en KT5Keystore, siga estos pasos:

1. Instale un agente Supervisión de tiempo de respuesta en cada servidor web HTTPS que desea supervisar.
2. Exporte un archivo .pfx desde Internet Information Services:
   a. En el menú **Inicio** de Windows, seleccione **Herramientas administrativas** > **Internet Information Services (IIS) Manager**.
   b. Seleccione el servidor web y sitio cuya clave privada desea exportar, a continuación pulse con el botón derecho del ratón y seleccione **Propiedades** en el menú contextual.
   c. Seleccione la pestaña **Seguridad del directorio** y a continuación seleccione **Certificado del servidor** en la sesión **Comunicaciones seguras**.
   d. En **Asistente de certificados de IIS**, pulse **Siguiente**.
   e. Seleccione **Exportar el certificado actual a un archivo .pfx** y pulse **Siguiente**.
   f. Especifique la vía de acceso y el nombre de archivo y pulse **Siguiente**.
   g. Especifique una contraseña de exportación para la clave y pulse **Siguiente**.
   h. Pulse **Siguiente** en todas las páginas subsiguiente y a continuación pulse **Finalizar**.
3. Extraiga los certificados personales y de firmante del archivo .pfx:

a. Ejecute **IBM Key Management** (iKeyman) desde el directorio `bin` de IBM Java utilizando el mandato `c:\IBM\APM\java\java80_x64\jre\bin\ikeyman`. Asegúrese de que esté establecida la variable de entorno `JAVA_HOME`.

b. En la base de datos del almacén de claves, seleccione **Archivo** > **Abrir**.

c. En la lista **Tipo de base de datos de claves**, seleccione **PKCS12**.

d. Especifique el nombre y la vía de acceso del archivo .pfx que ha creando anteriormente y a continuación pulse **Aceptar**. Cuando se le solicite, especifique la contraseña y a continuación pulse **Aceptar**.

e. Seleccione **Contenido de base de datos de claves** > **Certificados personales** y a continuación pulse **Exportar/Importar**.

f. Seleccione un tipo de acción de **Exportar clave** y un Tipo de archivo de clave de **PKCS12**. Especifique un nombre de archivo y una ubicación para la clave exportada y pulse **Aceptar**. Cuando se le solicite, especifique una contraseña de exportación y a continuación pulse de nuevo **Aceptar**.

g. Si el certificado personal lo ha firmado una entidad emisora de certificados, seleccione **Contenido de base de datos de claves** > **Certificados de firmante** y pulse **Extraer**. Seleccione el tipo de archivo predeterminado, especifique un nombre de archivo y ubicación para el certificado exportado y a continuación pulse **Aceptar**.

4. Extraiga los archivos `.cer` de firmante (si es necesario):

a. Si se ha extraído un archivo de certificados de firmante del archivo .pfx, vaya al directorio donde se ha guardado y realice una copia nueva con la extensión `.cer`. Pulse dos veces la copia nueva para abrirla utilizando el visor de certificados de Windows.

b. En la pestaña **Ruta de certificación** puede visualizar la cadena de certificado de firmante. El elemento más bajo de la cadena deberá ser el certificado personal. Para todos los certificados que hay sobre él, realice lo siguiente:

1) Seleccione un certificado y pulse **Ver certificado**.

2) Seleccione **Detalles** y pulse **Copiar en archivo**.

3) Acepte todos los valores predeterminados en el asistente de exportación de certificados y especifique un nombre de archivo con la extensión `.cer`.

5. Cree una base de datos del almacén de claves nueva. En el cuadro de diálogo **Nuevo**, complete los pasos siguientes:

a. En la lista **Tipo de base de datos de claves**, seleccione **CMS** y especifique un nombre de archivo y una ubicación. Cuando se le solicite, escriba una contraseña para el nuevo almacén de claves.

Nota: Asegúrese de seleccionar **¿Desea ocultar la contraseña en un archivo?**.

b. Si se han extraído certificados de firmante del archivo .pfx, realice lo siguiente:

1) Seleccione **Contenido de base de datos de claves** > **Certificados de firmante**.

2) Para cada certificado de firmante, pulse **Añadir** y añada el archivo `.cer`.

c. Seleccione **Contenido de base de datos de claves** > **Certificados personales** y pulse **Importar**.

d. Seleccione el tipo de archivo de claves **PKCS12** y el nombre y la ubicación del archivo **.p12**. Cuando se le solicite, escriba la contraseña.

e. Guarde el almacén de claves y salga del programa de utilidad de gestión de claves.

f. Copie los archivos `.kdb` y `.sth` en KT5Keystore en la máquina del dispositivo Supervisión de tiempo de respuesta.

g. Coloque los archivos de base de datos de IBM Key Management (`.kdb`) y stash (`.sth`) en un directorio seguro y asegúrese de que solo los pueda leer el usuario Administrador o `root` (o el ID de usuario utilizado para instalar el agente de Supervisión de tiempo de respuesta).

Configuración avanzada del Analizador de paquetes

Existen diversas opciones de configuración avanzada para el Analizador de paquetes.

Una vez que haya configurado el Analizador de paquetes, hay una serie de tareas de configuración avanzada que puede realizar para ajustar el rendimiento y las características.

Utilización de equilibradores de carga

Si utiliza equilibradores de carga en el entorno, deberá realizar algunos ajustes adicionales.

Procedimiento

Si está utilizando un equilibrador de carga, siga estas directrices:

1. Desactive la Reescritura de URL en el equilibrador de carga.
2. Instale un agente de Supervisión de tiempo de respuesta en cada servidor web que desee supervisar.

   No instale Supervisión de tiempo de respuesta en el equilibrador de carga.
3. Añada el componente de supervisión de JavaScript a la aplicación. Para obtener más información, consulte "Adición del componente de supervisión de JavaScript a la aplicación" en la página 730.

Qué hacer a continuación

Si está ejecutando el agente Supervisión de tiempo de respuesta tras un equilibrador de carga, puede configurar el equilibrador de carga para reenviar la dirección IP del cliente para optimizar el rendimiento de supervisión. Siga los pasos siguientes como ejemplo:

1. En la cabecera HTTP, establezca la dirección IP del cliente en el campo **`X-Forwarded-For`**.
2. Configure el agente Supervisión de tiempo de respuesta para utilizar la cabecera de dirección IP del cliente. Establezca la cabecera de dirección IP del cliente en el campo **`KFC_OVERRIDE_SOURCE_ADDR_HEADER`** en uno de los archivos siguientes en función del sistema operativo:
   - AIX Linux `/opt/ibm/apm/agent/tmaitm6/wrm/kfcmenv`
   - Windows `C:\IBM\ITM\TMAITM6_x64\wrm\Analyzer\kfcmenv`

   Por ejemplo:

   ```
   KFC_OVERRIDE_SOURCE_ADDR_HEADER=x-forwarded-for
   ```

   o si utiliza WebSEAL:

   ```
   KFC_OVERRIDE_SOURCE_ADDR_HEADER=iv-remote-address
   ```

Configuración del límite de sobrecarga de CPU

Si está operando en un entorno de carga de transacciones elevada, puede limitar los recursos de supervisión utilizados por el agente de Supervisión de tiempo de respuesta.

Acerca de esta tarea

Esta función limita el uso de CPU del agente de Supervisión de tiempo de respuesta supervisando e informando de solo una porción del tráfico web mediante el muestreo. El `Límite de sobrecarga de CPU` no está configurado de forma predeterminada. Debe configurar el `Límite de sobrecarga de CPU` en el servidor en el que el agente está instalado.

Procedimiento

Para configurar el `Límite de sobrecarga de CPU`, realice los pasos siguientes:

1. Abra el siguiente archivo en un editor de texto:

   Linux AIX `/opt/ibm/apm/agent/tmaitm6/wrm/kfcmenv`

   Windows `C:\IBM\ITM\TMAITM6_x64\wrm\Analyzer\kfcmenv`
2. Configure los valores para los parámetros siguientes:

KFC_MAX_PROTOCOL_PACKETRATE
La tasa de paquetes máxima inicial. Por ejemplo, si establece el parámetro como **KFC_MAX_PROTOCOL_PACKETRATE=2000**, la tasa de paquetes máxima es de 2000 paquetes por segundo. Esta tas varía dinámicamente en función del valor de **KFC_CPUTHROTTLE_TARGET** y el uso de CPU actual.

KFC_CPUTHROTTLE_TARGET
El porcentaje del recurso de CPU global que el proceso `kfcmserver` puede utilizar. Por ejemplo, si establece el parámetro como **KFC_CPUTHROTTLE_TARGET=10.0**, el proceso `kfcmserver` puede utilizar hasta el 10% del recurso de CPU general.

Nota: El valor del parámetro **KFC_CPUTHROTTLE_TARGET** es el porcentaje del recurso de CPU general que está disponible para el proceso `kfcmserver`. Por ejemplo, si tiene 4 núcleos de CPU y **KFC_CPUTHROTTLE_TARGET** está establecido en 10, el supervisor de recursos en Windows mide el recurso de CPU como 400 %. Como resultado, el proceso `kfcmserver` puede utilizar hasta can el 40% de los recursos de total del 400% de recursos de CPU.

Resultados
Se ha configurado el `Límite de sobrecarga de CPU` para el agente de Supervisión de tiempo de respuesta.

Reconfiguración del módulo Tiempo de respuesta de IBM HTTP Server al Analizador de paquetes

Es posible que desee cambiar el entorno de supervisión del módulo Tiempo de respuesta de IBM HTTP Server por el Analizador de paquetes.

Procedimiento

1. Desinstale el agente de HTTP Server
   a) Edite `/etc/httpd/conf/httpd.conf` comentando la línea del plug-in de Tiempo de respuesta. Por ejemplo:

   ```
   #include /opt/ibm/apm/agent/tmp/khu/khu.etc.httpd.conf.httpd.conf
   ```

   b) Desinstale el agente de HTTP Server. Por ejemplo:

   ```
   /opt/ibm/apm/agent/bin/http_server-agent.sh uninstall
   ```

   c) Abra una ventana de indicador de mandatos nueva para limpiar la variable del sistema antes de volver a configurar el agente de Tiempo de respuesta en el paso siguiente.
2. Abrir el archivo siguiente

   Linux AIX *dir_instalación*`/config/`*nombre_host*`_t5.cfg`
   Donde *dir_instalación* es `/opt/ibm/apm/agent`
   Windows *dir_instalación*`\TMAITM6_x64\`*nombre_host*`_t5.cfg`
   donde *dir_instalación* es `C:\IBM\APM`
3. Defina los parámetros del modo siguiente:

   ```
   { KT5DISABLEANALYZER=NO } { KT5ENABLEWEBPLUGIN=NO }
   ```

4. Vuelva a configurar el agente como se indica a continuación:

   ```
   re-agent.bat config  dir_instalación\samples\rt_silent_config.txt
   ```

Personalización de valores de ubicación de transacciones de usuario final

Puede personalizar las ubicaciones aplicadas a direcciones IP específicas o rangos de direcciones en los paneles de instrumentos Transacciones de usuario final para su entorno concreto.

Antes de empezar

Utilice la pestaña **Geolocalización** en la **Configuración de agente** para personalizar los valores de ubicación.

Utilice esta característica para establecer la ubicación de las direcciones IP que se visualizan en el panel de instrumentos como **Desconocido**. Estas direcciones pueden ser direcciones internas, por ejemplo `192.168.x.x` o `10.x.x.x`, o direcciones IP externas que no están resueltas. También puede utilizar esta característica para alterar temporalmente ubicaciones incorrectas para las direcciones IP. Por ejemplo, si sabe que la dirección IP `9.1.1.1` está en Los Angeles, pero se muestra como San Francisco, altere temporalmente la ubicación, y establezca `9.1.1.1` para Los Angeles.

Acerca de esta tarea

Personalice los valores de ubicación en los paneles de instrumentos Transacciones de usuario final cargando un archivo CSV que contenga los valores que se requieran. Puede encontrar un archivo CSV de ejemplo en la pestaña **Geolocalización**.

El archivo CSV debe tener los valores siguientes como cabecera. Los valores pueden estar en cualquier orden y las entradas deben coincidir con ese orden.

```
IP_ADDRESS, COUNTRY, REGION, CITY
```

Por ejemplo,

```
IP_ADDRESS, COUNTRY, REGION, CITY
10.0.5.0/24, Australia, WA, Perth
10.1.0.6, Australia, VIC, Melbourne
```

Puede especificar una sola dirección IPv4, o un rango. Si especifica un rango, asegúrese de que utiliza un valor válido en el rango 1-32.

Procedimiento

Para personalizar los valores de ubicación visualizados en los paneles de instrumentos Transacciones de usuario final, realice los pasos siguientes en el panel de instrumentos Rendimiento de aplicación.

1. Configure el archivo o archivos CSV, con direcciones IP coincidentes con ubicaciones.
2. Cargue el archivo CSV.
   a) Vaya a **Configuración de agente** > **Geolocalización**.
   b) Pulse **Cargar CSV**, seleccione los archivos que desee cargar y pulse **Abrir**.
      - Asegúrese de que el archivo CSV liste primero los rangos de direcciones IP generales, antes de direcciones IP más específicas.
      - Cargue varios archivos, si es necesario.
      - Si los valores de un archivo se solapan con los de otro, los valores del archivo más nuevo sustituirán los valores del primer archivo.
3. Expanda **Cargar resultados** para comprobar si hay errores. Compruebe los posibles problemas siguientes:
   - Alteraciones temporales
   - Direcciones IP no válidas
   - Filas no válidas
   - Valores con más de 250 caracteres

Resultados

Espere algunos minutos y visualice los valores personalizados en los paneles de instrumentos Transacciones de usuario final.

Qué hacer a continuación

Puede eliminar valores personalizados, si es necesario. Complete uno de los pasos siguientes:

- Para eliminar algunos de los valores personalizados, seleccione las direcciones IP que desee eliminar, pulse **Borrar las entradas seleccionadas** y pulse **Aceptar** para confirmar la eliminación.
- Para eliminar todos los valores personalizados, pulse **Borrar todas las entradas** y pulse **Aceptar** para confirmar la eliminación.

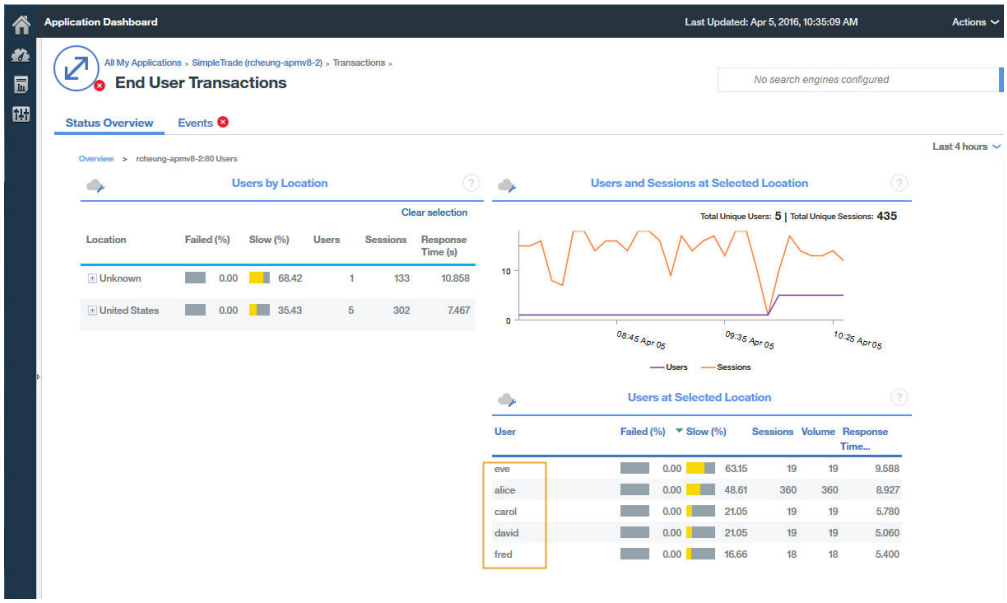
Rastreo de aplicaciones web adicionales

Para rastrear aplicaciones web además de las que se rastrean de forma predeterminada, debe identificar y configurar métodos de rastreo de usuarios y sesiones.

Antes de empezar

Si la aplicación no está soportada por los valores predeterminados, los paneles de instrumentos no contienen detalles de usuario y sesión, el nombre de usuario se visualiza como `anónimo` o `desconocido`, y no hay disponible información de sesión.

Si los métodos de rastreo se configuran correctamente, el ID de usuario se extrae y se lista en el panel de instrumentos **Transacciones de usuario final** > **Resumen de usuarios** > **Usuarios de ubicaciones seleccionadas**.



Nota: el rastreo de usuarios se basa en el rastreo de sesiones. Debe establecer primero la variable de métodos de rastreo de sesiones correcta, en los valores de configuración del agente de tiempo de respuesta, para los métodos de rastreo de usuarios y sesiones.

Acerca de esta tarea

En IBM Application Performance Management V8.1.4 y posteriores, puede utilizar la página **Configuración de agente** > **Tiempo de respuesta** para añadir aplicaciones a rastrear mediante el Analizador de paquetes o el Módulo de Tiempo de respuesta de IBM HTTP Server. Los valores definidos en esta página tienen preferencia sobre los valores definidos en el archivo `WRT_Defaults.xml`.

Para rastrear aplicaciones adicionales, primero debe identificar los métodos y valores de ID de usuario e ID de sesión para la aplicación que desea supervisar. Por ejemplo:

1. Abra la herramienta del desarrollador correspondiente a su navegador, a fin de ver las solicitudes de la aplicación que desea supervisar.
2. Seleccione la última solicitud en el registro de red del navegador, a fin de identificar la solicitud de prueba con facilidad.

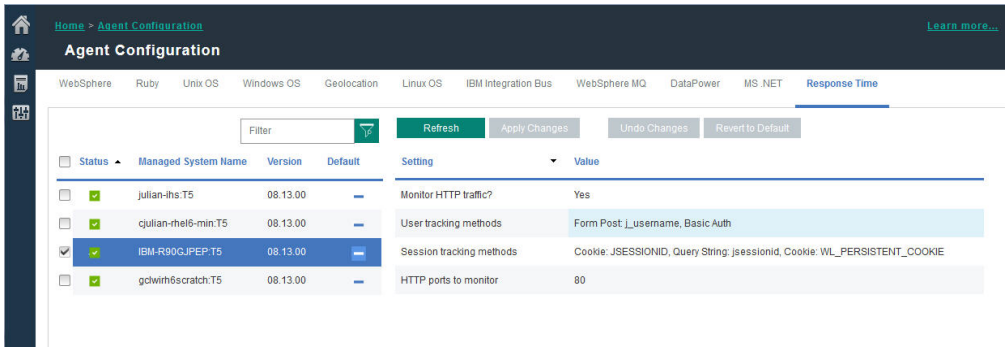
3. Cree una solicitud de prueba con parámetros que reconozca. Por ejemplo, inicie la sesión en su sitio web con `testuser`.
4. Seleccione la solicitud de prueba y observe `Cabeceras`.
5. Identifique el ID de sesión del registro de solicitud. El ID de sesión se especifica habitualmente en `cookie`, `POST`, `request/response header` o `query string`. Si `cookie` ya se ha definido en el perfil predeterminado, no es necesario añadirlo en el paso 2.
6. Identifique el ID de usuario del registro de solicitud. El ID de usuario puede especificarse en el contenido de `cookie`, `request header`, `POST` o `query string`. Por ejemplo, busque `testuser`, que le dará el valor del ID de usuario.
7. Tanto los **Métodos de rastreo de usuarios** como los **Métodos de rastreo de sesiones** deben actualizarse con el nombre de valor de usuario y sesión correctos utilizados en el código de aplicación del cliente. La forma de identificar el nombre de valor de la sesión y el nombre de usuario depende del código de aplicación. A continuación se muestra el valor predeterminado del valor de Usuario/Sesión en 8.1.4.

```
Session tracking methods=cookie\:JSESSIONID,querystring\:jsessionid,cookie\
       :WL_PERSISTENT_COOKIE
User tracking methods=formpost\:j_username,formpost\:uid,formpost\
       :ctl00%24MainContent%24uid,basicauth\:Authorization\: Basic
```

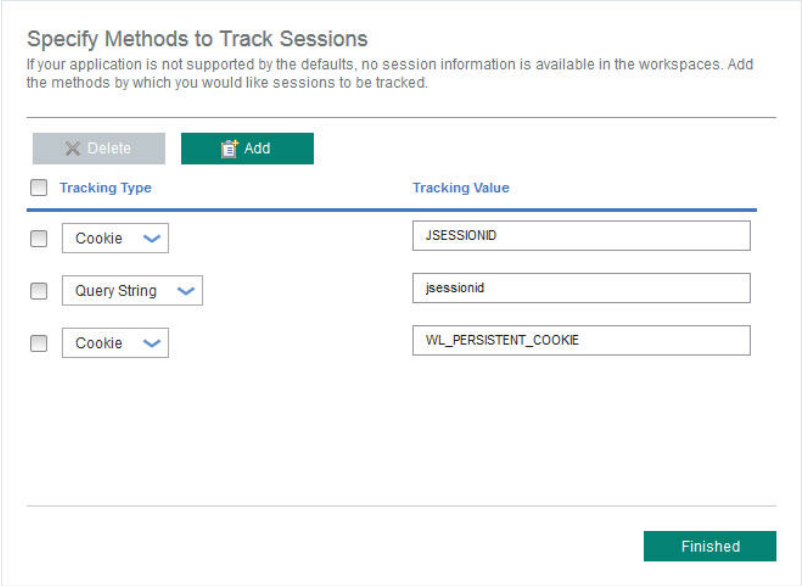
Procedimiento

Después de haber identificado los métodos de rastreo de usuarios y sesiones utilizados en la aplicación, complete los pasos siguientes:

1. Vaya a la página **Configuración de agente** > **Tiempo de respuesta**.



2. Seleccione el sistema gestionado que desea actualizar.
3. Si es necesario, actualice los métodos de rastreo de sesión:
   a) Pulse el valor del campo **Métodos de rastreo de sesión**.



b) En la ventana **Especificar métodos para realizar el seguimiento de sesiones**, pulse **Añadir**.

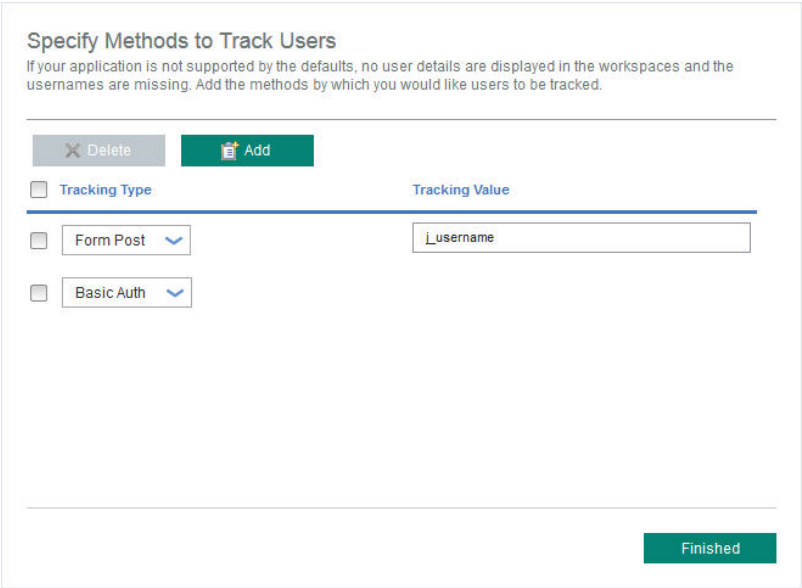
c) En la lista **Tipo de rastreo**, seleccione el tipo de rastreo. Por ejemplo, `Cookie`.

d) En el campo **Valor de rastreo**, especifique un valor. Por ejemplo, `WL_PERSISTENT_COOKIE`.

e) Pulse **Finalizado**.

4. Si es necesario, actualice los métodos de rastreo de usuarios:

a) Pulse el valor del campo **Métodos de rastreo de usuario**.



b) En la ventana **Especificar métodos para realizar el seguimiento de usuarios**, pulse **Añadir**.

c) En la lista **Tipo de rastreo**, seleccione el tipo de rastreo. Por ejemplo, `Cabecera`.

d) En el campo **Valor de rastreo**, especifique un valor. Por ejemplo, `username`.

e) Pulse **Finalizado**.

5. En la página de configuración del agente, pulse **Aplicar cambios**.

Resultados

Las aplicaciones que utilizan los métodos de rastreo recién especificados se visualizan en el panel de instrumentos de aplicaciones.

Qué hacer a continuación
Compruebe que la información de ID de usuario y sesión de la aplicación se visualiza en el panel de instrumentos de aplicaciones.

Especificación de un nombre de sistema gestionado exclusivo para el Agente de Supervisión de tiempo de respuesta

El nombre de instancia de Agente de Supervisión de tiempo de respuesta que se visualiza en la consola de Cloud APM se conoce también como nombre de sistema gestionado (MSN). Puede utilizar el parámetro de configuración del agente para especificar un MSN exclusivo para cada instancia de agente.

Acerca de esta tarea
El nombre del sistema gestionado para el Agente de Supervisión de tiempo de respuesta está en el formato siguiente:

```
nombre_instancia:nombre_host:T5
```

T5 es el código de producto para el Agente de Supervisión de tiempo de respuesta.

Procedimiento

1. Detenga todas las instancias de agente. Si no tiene ninguna instancias de agente existente, continúe con el paso siguiente. Para obtener más información sobre cómo detener instancias de agente, consulte "Utilización de mandatos de agente" en la página 184.
2. Linux AIX Cambie **CTIRA_SUBSYSTEM_ID** en el archivo `runagent`. Normalmente, todas las instancias de agente de una máquina utilizan el mismo valor de nombre de host.
   a) Haga una copia de seguridad del archivo:

   Linux AIX
   ```
   dir_instalación/plataforma/t5/bin/runagent
   ```

   b) Edite el archivo. Añada *nuevo_nombre_instancia* en sistemas Linux o AIX.

   Linux AIX
   ```
   CTIRA_SUBSYSTEM_ID=nuevo_id_subsistema
   ```
3. Inicie las instancias existentes del agente.
4. Inicie Consola de Cloud APM. Modifique sus aplicaciones eliminando las instancias de agente bajo los MSN antiguos y añadiendo el las nuevas instancia de agente.

Configuración de la supervisión de Ruby

Puede supervisar aplicaciones Ruby locales y de IBM Cloud. Para supervisar aplicaciones Ruby locales, configure el Agente de Ruby. Para supervisar aplicaciones Ruby de IBM Cloud configure el Recopilador de datos de Ruby.

Acerca de esta tarea

Las instrucciones son para el release más reciente del agente, a excepción de lo indicado.

El procedimiento siguiente es una hoja de ruta para configurar el Agente de Ruby y el Recopilador de datos de Ruby que incluye pasos obligatorios y opcionales. Siga los pasos de configuración según sus necesidades.

Procedimiento

- Para supervisar las aplicaciones Ruby locales, siga estos pasos para configurar el Agente de Ruby:
  a) Configure las instancias de agente para supervisar aplicaciones Ruby. Consulte Configuración del Agente de Ruby para supervisar aplicaciones Ruby.

b) Instale el recopilador de datos para datos de supervisión que deben visualizarse en la Consola de Cloud APM. Consulte la sección Instalación del recopilador de datos.

c) Opcional: Si es usuario de Cloud APM, Advanced, puede realizar las tareas siguientes según sus necesidades:

- Para configurar el recopilador de datos para recopilar datos de diagnóstico, consulte la sección Configuración del recopilador de datos de diagnóstico.
- Para habilitar el rastreo de método y ajustar la longitud del parámetro de vía de acceso de archivo que se visualiza en el widget Seguimiento de pila de solicitudes, consulte la sección Habilitación del rastreo de método y ajuste de la visualización de vía de acceso.
- Para aumentar el tamaño del almacenamiento intermedio de JVM para evitar errores de `memoria insuficiente`, consulte la sección Aumento del tamaño de almacenamiento dinámico de JVM.
- Para inhabilitar los diagnósticos, consulte la sección Inhabilitación o habilitación de datos de diagnóstico para aplicaciones Ruby.

- Para supervisar las aplicaciones Ruby de IBM Cloud, realice estas tareas para configurar el Recopilador de datos de Ruby:

a) Configure el recopilador de datos de Ruby para aplicaciones IBM Cloud. Para obtener instrucciones, consulte "Configuración del Recopilador de datos de Ruby para aplicaciones de IBM Cloud" en la página 751.

b) Opcional: Para cambiar el comportamiento del recopilador de datos de Ruby, consulte "Personalización del Recopilador de datos de Ruby para aplicaciones IBM Cloud" en la página 752.

Configuración del Agente de Ruby

Para que el Agente de Ruby supervise las aplicaciones, especifique el tiempo de ejecución de Ruby. Como resultado, utilizará el tiempo de ejecución para recopilar datos de las aplicaciones Ruby y configurar el agente.

Antes de empezar

Determine el servidor que se utiliza para iniciar aplicaciones Ruby y el directorio bin calificado para el ejecutable de Ruby o Rake utilizado por el agente:

1. Para determinar el servidor de aplicaciones que está utilizando, ejecute el mandato siguiente:

```
ps -ef | grep ruby
```

Verá el nombre del servidor utilizado para iniciar la aplicación. Los nombres de servidor posibles se listan del siguiente modo:

- `Passenger`
- `Unicorn`
- `Puma`
- `Thin`

Si la salida del mandato no indica los nombres de servidor que se muestran en la lista anterior, el servidor utilizado para iniciar la aplicación puede ser WEBrick.

Importante: si utiliza varias servidores web para iniciar las aplicaciones Ruby, debe crear una instancia de agente para cada servidor web de aplicaciones, por ejemplo, una instancia para PUMA y una para Unicorn.

2. Para determinar el directorio bin calificado para el ejecutable de Ruby o Rake utilizado por el Agente de Ruby, ejecute el mandato siguiente:

```
which ruby
```

Acerca de esta tarea
Puede repetir esta tarea para configurar varias instancias de agente según sus necesidades.

Procedimiento

1. Para configurar el agente, ejecute el mandato siguiente:
   dir_instalación/bin/ruby-agent.sh config *nombre_instancia*
   donde *nombre_instancia* es el nombre que desea dar a la instancia, y *dir_instalación* es el directorio de instalación del Agente de Ruby. El directorio de instalación predeterminado es /opt/ibm/apm/agent.

   Importante: No especifique un nombre de instancia largo. La longitud total del nombre de host y el nombre de instancia de agente no debe superar los 28 caracteres. Si la longitud supera el límite, el Nombre de sistema gestionado queda truncado y el código de producto del Agente de Ruby no se visualiza correctamente.

   El Nombre de sistema gestionado incluye el nombre de instancia que especifique, por ejemplo, *nombre_instancia*:*nombre_host*:*pc*, donde *pc* es el código de producto de dos caracteres para el agente. Por ejemplo, si especifica Ruby2 como nombre de instancia, el nombre de sistema gestionado será Ruby2:nombrehost:KM, donde *KM* es el código de producto de dos caracteres del Agente de Ruby.
2. Cuando se le solicite Editar valores de 'Monitoring Agent for Ruby', especifique 1 para continuar.
3. Cuando se le solicite el directorio Bin de Ruby completo, especifique el directorio binario. Por ejemplo, si utiliza Ruby Version Manager (RVM), especifique /usr/local/rvm/rubies/ruby-2.0.0-p247/bin.
4. Cuando se le solicite Detectar automáticamente indicador de aplicaciones Ruby, especifique Y para continuar. El agente recibe los datos enviados por el recopilador de datos de agentes.
5. Cuando se le solicite el nombre de proceso de servidor de aplicaciones, pulse Intro para aceptar el valor predeterminado ruby o especifique el valor del servidor que usa conforme a la lista siguiente:
   - Para los servidores WEBrick, acepte el valor predeterminado o especifique ruby; si Rails está instalado por Ruby Stack, especifique .ruby.bin.
   - Para los servidores Passenger, especifique passenger.
   - Para los servidores Unicorn, especifique unicorn.
   - Para los servidores Puma, especifique puma.
   - Para los servidores Thin, si las aplicaciones se han iniciado mediante el mandato thin start, acepte el valor predeterminado para usar ruby; si las aplicaciones se han iniciado mediante el mandato thin start -d, especifique thin; si Rails está instalado por Ruby Stack y las aplicaciones se han iniciado ejecutando el mandato thin start, especifique .ruby.bin.
6. Cuando se le solicite el origen de datos de socket, pulse Intro para aceptar el valor predeterminado de 0 y utilizar el puerto efímero.
7. Cuando se le solicite Editar valores de 'Aplicación', especifique 5 para salir.
8. Para iniciar el agente, ejecute el mandato siguiente:
   dir_instalación/bin/ruby-agent.sh start *nombre_instancia*

Qué hacer a continuación
Instale el recopilador de datos para que el Agente de Ruby funcione adecuadamente y para que los datos se visualicen en la IU de Cloud APM. Para obtener instrucciones, consulte la sección Instalación del recopilador de datos

Instalación del recopilador de datos
Debe instalar el recopilador de datos para que el agente funcione adecuadamente. Tras instalar el recopilador de datos, los datos de supervisión se visualizarán en el Panel de instrumentos del rendimiento de aplicaciones.

Antes de empezar
Si ha instalado la aplicación Ruby on Rails en un sistema Linux utilizando una cuenta no root, y tiene previsto recopilar datos de diagnósticos, el usuario no root debe tener acceso al directorio de inicio del recopilador de datos de diagnósticos. Compruebe que el usuario no root tenga acceso de lectura y grabación al directorio *dir_instalación*/install-images/kkm donde *dir_instalación* es el directorio de instalación de Agente de Ruby. El directorio de instalación predeterminado es /opt/ibm/apm/agent. Si es necesario, otorgue permisos de lectura y grabación mediante el mandato chmod 777.

Procedimiento

1. Detenga la aplicación Ruby on Rails.
2. Opcional: Si está actualizando el recopilador de datos Ruby a una versión nueva, primero debe desinstalar el recopilador de datos de la versión anterior ejecutando el mandato siguiente:

   ```
   gem uninstall stacktracer
   ```

3. Instale el recopilador de datos de diagnóstico. Especifique gem install --local *dir_instalación*/lx8266/km/bin/stacktracer-*versión*.gem, donde *versión* es el número de versión, y *dir_instalación* es el directorio de instalación de Agente de Ruby. El número de versión del nombre del archivo stacktracer-*versión*.gem del directorio de instalación del agente indica el número de versión que debe especificar aquí. El directorio de instalación predeterminado es /opt/ibm/apm/agent.

   Importante: instale el recopilador de datos con el mismo usuario que ha utilizado para instalar y ejecutar la aplicación Ruby on Rails.
4. Vaya al directorio de inicio de la aplicación, abra su Gemfile y añada la línea siguiente al final del archivo: gem 'stacktracer', '*versión*'
   donde *versión* es el número de versión del recopilador de datos. El número de versión se indica en el nombre del archivo stacktracer-*versión*.gem que está en el *dir_instalación* del Agente de Ruby. Por ejemplo, si instala el recopilador de datos Ruby Versión 1.0 Fix Pack 8, puede encontrar un archivo stacktracer-01.00.08.00.gem en el directorio de instalación del agente. A continuación, añada la línea gem 'stacktracer', '01.00.08.00' a la aplicación para instalar el recopilador de datos.

   Nota: si solo hay una versión de stacktracer en el entorno, añada la línea gem 'stacktracer' hasta el final del archivo. No especifique el número de versión de la línea.
5. En el directorio de inicio de la aplicación, especifique bundle install.
6. Reinicie la aplicación Ruby on Rails.

Resultados
El recopilador de datos se ha instalado y configurado y se inicia la aplicación Ruby on Rails.

Qué hacer a continuación

- Si no ha iniciado sesión, siga las instrucciones en "Inicio de la Consola de Cloud APM" en la página 1009. Seleccione **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** para abrir el panel de instrumentos **Todas mis aplicaciones** y profundizar en los paneles de instrumentos de diagnóstico y de supervisión de recursos de aplicación Ruby on Rails para observar las aplicaciones Ruby on Rails desde el resumen de estado hasta detalles de solicitud individual.
- Para ver y modificar los valores del recopilador de datos de diagnóstico, continúe en el tema siguiente, "Configuración del recopilador de datos de diagnóstico" en la página 747.

- Para visualizar datos de rastreo de método en la IU de Cloud APM, consulte la sección Habilitación del rastreo de método y ajuste de la visualización de vía de acceso.
- Cuando el rastreo de método o las solicitudes de datos son de gran tamaño, puede que reciba errores de tipo `sin memoria`. Puede aumentar el tamaño de almacenamiento dinámico de JVM para evitarlos. Consulte la sección Aumento del tamaño de almacenamiento dinámico de JVM.
- Puede inhabilitar y habilitar la recopilación de datos de diagnóstico para una o más aplicaciones Ruby on Rails gestionadas en cualquier momento a través de la Consola de Cloud APM. Consulte "Inhabilitación o habilitación de datos de diagnóstico para aplicaciones Ruby" en la página 751. Esta función no está disponible para la supervisión de recursos.

Configuración del recopilador de datos de diagnóstico
Si es un usuario de Cloud APM, Advanced, puede seguir configurando el recopilador de datos para datos de diagnóstico. La recopilación de datos de diagnóstico está inhabilitada de forma predeterminada en el archivo de configuración del recopilador de datos.

Antes de empezar
Debe tener instalado el recopilador de datos de diagnóstico y configurado el soporte para la recopilación de datos de diagnóstico, tal como se describe en "Instalación del recopilador de datos" en la página 746.

Acerca de esta tarea
El archivo de configuración `instrumenter_settings.rb` aparece después de que el agente registre la existencia de una aplicación Ruby on Rails configurando adecuadamente el `Gemfile`. Este archivo de configuración se puede modificar mientras el agente Ruby se está ejecutando, y los cambios se recogen automáticamente. De forma alternativa, puede aplicar los cambios a todas las aplicaciones Ruby on Rails que se están supervisando, lo cual requiere detener las aplicaciones mientras se edita el archivo de configuración.

Procedimiento

- Para modificar los valores del recopilador de datos de una aplicación específica en ejecución:
  1. Vaya al directorio *dir_instalación*`/install-images/kkm/dchome/`*nombreClaseAplic*`/config`, donde *nombreClaseAplic* es el nombre de clase de aplicación Ruby, y *dir_instalación* es el directorio de instalación de Agente de Ruby. El directorio de instalación predeterminado es `/opt/ibm/apm/agent`.
  2. Abra `instrumenter_settings.rb` en un editor de texto.
  3. Modifique los valores del recopilador de datos:

     :instrumentation_enabled
     Para habilitar el soporte para la recopilación de datos de diagnóstico, establezca `:instrumentation_enabled => true`.

     Para inhabilitar el soporte para la recopilación de datos de diagnóstico, establezca `:instrumentation_enabled => false`.

     :sample_frequency
     Para modificar la frecuencia de muestreo de las solicitudes, especifique el número de solicitudes entre muestreos.

     El recopilador de datos recopila datos de diagnóstico solo para solicitudes muestreadas. Si establece `:sample_frequency => 10`, por ejemplo, los datos se recopilan para 1 de cada 10 solicitudes.

     :max_methods_to_instrument
     Para inhabilitar la recopilación de rastreo de método o habilitar la recopilación de rastreo de método y limitar el número de métodos que se rastrean, establezca el valor en cero o especifique el número máximo de métodos a rastrear.

     Para inhabilitar la recopilación de rastreos de método, establezca `:max_methods_to_instrument => 0`.

Para habilitar la recopilación de rastreos de método, establezca `:max_methods_to_instrument => 10000`. El valor puede ser superior, pero un valor mucho mayor puede provocar problemas de rendimiento. Cuando se recopilan datos de método, las llamadas a los métodos se incluyen en el widget Rastreo de método del panel de instrumentos Rastreos de solicitud, que muestra todas las instancias de solicitud y sus solicitudes anidadas.

:min_wallclock_to_include_in_trace
Para modificar el umbral que determina si debe rastrearse la solicitud o el método, establezca el tiempo de respuesta mínimo. Si establece `:min_wallclock_to_include_in_trace => 0,001`, por ejemplo, sólo se rastrearán las solicitudes y métodos cuyos tiempos de respuesta sean superiores a 1 milisegundo.

Recuerde: En el panel de instrumentos de diagnóstico **Rastreo de solicitud**, puede detallar más hasta una instancia de solicitud específica desde el widget de grupo Seguimiento de la pila de solicitudes. Los totales de los tiempos de respuesta para la instancia pueden ser incorrectos debido a los filtros establecidos para `:min_wallclock_to_include_in_trace` y `:min_wallclock_to_include_stacks`, que pueden excluir algunos datos.

:min_wallclock_to_include_stacks
Para modificar el umbral que determina si debe recopilarse la información de seguimiento de la pila para una solicitud o de método, establezca el tiempo de respuesta mínimo.

Si establece `:min_wallclock_to_include_stacks => 0,1`, por ejemplo, la información de seguimiento de la pila se recoge para todas las solicitudes y métodos cuyo tiempo de respuesta es superior a 100 milisegundos.

:include_subclasses_of_these_modules
El panel de instrumentos Rastreos de solicitud ayuda a identificar la secuencia de llamadas a solicitudes y métodos anidados para una instancia de solicitud. El recopilador de datos filtra de forma preventiva los métodos de las clases que no están incluidas en la lista de filtros. Si las operaciones que desea rastrear no están incluidas en los rastreos de pila de método, puede añadirlas aquí.

Para especificar los métodos que deben rastrearse, añada sus nombres de clase.

Considere, por ejemplo, que desea rastrear las API Moped en el siguiente tipo de código Ruby:

```
session = Moped::Session.new(['ip:27017'])
session.use(:HR)
session[:profiles].insert({......})
session[:profiles].find({...}).remove
```

Añada los nombres de módulo de estas API Moped a la propiedad:

```
:include_subclasses_of_these_modules => {"
ActionController" => true,
                     "ERB" => true,
                     "erb" => true,
                     "Arel" => true,
                     "Mongoid" => true,
                     "Moped" => true
                    },
```

Restricción: Los rastreos de método no incluyen métodos de clase y métodos privados (métodos definidos en una clase que tienen especificadores de acceso "privados" implícitos o explícitos).

:include_sql_text
Para recopilar datos de contexto para los métodos, establezca esta propiedad en `true`.

:num_samples_per_file
Para modificar el número máximo de solicitudes rastreadas que deben almacenarse en cada archivo, especifique un valor como `:num_samples_per_file => 1000`. Una vez alcanzado el límite establecido aquí, se crea un archivo.

Considere la posibilidad de establecer `:num_samples_per_file` en un valor inferior si ajusta la configuración de tal forma que provoca la recopilación de más datos. Por ejemplo, al establecer que `:include_subclasses_of_these_modules` para rastrear más clases y métodos, aumenta la recopilación de datos. Al establecer cualquiera de las propiedades siguientes en un valor inferior, también puede aumentar la recopilación de datos: `:sample_frequency`, `:min_wallclock_to_include_in_trace` y `:min_wallclock_to_include_stacks`.

:verbose_request_instrumentation
:verbose_class_instrumentation
:verbose_method_instrumentation
Para aumentar el nivel de registro del recopilador de datos de diagnóstico, establezca estas propiedades en `true`.

Consejo: Si las operaciones que desea rastrear específicamente no están incluidas en los seguimientos de la pila de método, establezca `:verbose_class_instrumentation => true` y compruebe el registro para averiguar si la clase que desea rastrear está instrumentada. Si no está instrumentada, añada el nombre de clase del nombre de módulo de la clase a la propiedad `:include_subclasses_of_these_modules`.

4. Si ha editado alguna de las propiedades siguientes, reinicie la aplicación Ruby on Rails correspondiente para que los cambios entren en vigor:

```
:include_subclasses_of_these_modules
:max_methods_to_instrument
```

El reinicio es necesario porque estas propiedades se utilizan sólo cuando se lanza una aplicación para determinar qué clase o método debe instrumentar el recopilador de datos de Ruby.

- Para modificar los valores del recopilador de datos de todas las aplicaciones Ruby on Rails, complete estos pasos:
  1. Detenga las aplicaciones Ruby on Rails que se estén ejecutando.
  2. Elimine `instrumer_settings.rb` del directorio *`dir_instalación`*`/install-images/kkm/dchome/`*`nombre_aplicación`*`/config`.
  3. Modifique los valores del recopilador de datos en *`dir_Gem`*`/gems/stacktracer-`*`versión`*`/config/instrumenter_settings_template.rb` donde *versión* es el número de versión, como por ejemplo 01.00.05.00 y *dir_Gem* es el directorio de instalación de `stacktracer-version.gem`, como por ejemplo `/usr/local/rvm/gems/ruby-2.1.4/`. Para obtener más información, consulte el paso “3” en la página 747 en el procedimiento para modificar los valores del recopilador de datos de una aplicación específica.
  4. Reinicie las aplicaciones Ruby on Rails que se estén ejecutando.

Resultados
La configuración del recopilador de datos de diagnóstico ha cambiado para la aplicación en ejecución especificada o para todas las aplicaciones.

Habilitación del rastreo de método y ajuste de la visualización de la vía de acceso
IBM Cloud Application Performance Management, Advanced con datos de diagnóstico permite a los usuarios disponer de un panel de instrumentos **Rastreos de solicitud**. Si se recopilan datos de método, se muestran las llamadas a métodos. El widget **Rastreo de método** muestra instancias de solicitud y sus solicitudes anidadas. Puede habilitar el rastreo de métodos para incluir llamadas a métodos en las solicitudes anidadas. También puede ajustar la configuración del widget **Seguimiento de la pila de solicitudes** para que muestre más caracteres que los 50 predeterminados de cada vía de acceso de archivo.

Acerca de esta tarea
El rastreo de método está inhabilitado de forma predeterminada. Complete el primer procedimiento para habilitar el rastreo de método a fin de visualizarlo en el panel de instrumentos **Rastreos de solicitud**. Puede habilitar el rastreo de método cambiando un valor en el archivo de configuración.

Complete el segundo procedimiento para ajustar el número de caracteres que se muestran en la vía de acceso de archivo en el widget **Seguimiento de la pila de solicitudes**.

Procedimiento

- Para habilitar el rastreo de método, edite los valores de `instrumenter_settings.rb`:
  a) Busque el archivo `instrumenter_settings.rb` en la instalación de Agente de Ruby, por ejemplo, *`dir_instalación`*`/install-images/kkm/dchome/`*`appClassName`*`/config` donde *appClassName* es el nombre de clase de aplicación Ruby y *dir_instalación* es el directorio de instalación de Agente de Ruby. El directorio de instalación predeterminado es `/opt/ibm/apm/agent`.
  b) Abra `instrumenter_settings.rb` en un editor de texto.
  c) Establezca la propiedad siguiente en 10000.

  ```
  max_method_to_instrument
  ```

  El valor puede ser superior, pero un valor mucho mayor puede provocar problemas de rendimiento. (Consulte también el apartado "Aumento del tamaño de almacenamiento dinámico de la JVM" en la página 750.)
  d) Reinicie las aplicaciones Ruby on Rails para empezar la recopilación de datos de método.

  Para obtener más información sobre todas las propiedades de `instrumenter_settings.rb`, consulte "Configuración del recopilador de datos de diagnóstico" en la página 747.
- Para ajustar el tamaño de visualización de la vía de acceso de archivo en el widget **Seguimiento de la pila de solicitudes**, edite el archivo `dfe.properties`:
  a) Busque el archivo `dfe.properties` en la instalación de Agente de Ruby por ejemplo, *`dir_instalación`*`/lx8266/km/bin/dfe.properties`
  donde *dir_instalación* es el directorio de instalación de Agente de Ruby. El directorio de instalación predeterminado es `/opt/ibm/apm/agent`.
  b) Abra `dfe.properties` en un editor de texto.
  c) Cambie el tamaño máximo de la vía de acceso del archivo que debe visualizarse en cada elemento de seguimiento de la pila ajustando el valor de la propiedad siguiente:

  ```
  dfe.stacktrace.filepath.maxsize
  ```

  d) Reinicie el Agente de Ruby.

Aumento del tamaño de almacenamiento dinámico de la JVM
Cuando el rastreo de método está habilitada para el panel de instrumentos de diagnósticos de Ruby **Rastreos de solicitud** o las solicitudes de datos son muy grandes, puede aumentar el tamaño de almacenamiento dinámico de JVM para evitar errores de falta de memoria.

Acerca de esta tarea

Agente de Ruby es un agente basado en Java y el tamaño de almacenamiento dinámico es de 384 MB. Siga estos pasos para aumentar el tamaño del almacenamiento dinámico y así reducir la probabilidad de la condición de falta de memoria. La condición de memoria insuficiente se puede producir a partir de solicitudes de datos grandes y cuando tenga el rastreo de método activado.

Procedimiento

1. Busque el valor de tamaño de almacenamiento dinámico de JVM en el directorio de instalación del Agente de Ruby, por ejemplo, *`dir_instalación`*`/lx8266/km/bin/runDeepDiveClient.sh`
   Donde *dir_instalación* es el directorio de instalación del Agente de Ruby. El directorio de instalación predeterminado es `/opt/ibm/apm/agent`.
   El valor predeterminado es `-Xmx384m`.
2. Aumente el valor, por ejemplo a 1024 MB, mostrado como `-Xmx1024m`:

```
export JAVA_OPT="-Djlog.common.dir=$CANDLEHOME/logs -DCONFIG_DIR=
$DC_RUNTIME_DIR -Dkqe.cache.interval=60 -Xmx1024m -Dkqe.timespan=900 -
Djlog.propertyFileDir.CYN=$CANDLEHOME/$ITM_BINARCH/$PRODUCT_CODE/bin"
```

3. Reinicie el Agente de Ruby.

Inhabilitación o habilitación de datos de diagnóstico para aplicaciones Ruby
Si tiene IBM Cloud Application Performance Management, Advanced, puede utilizar la página **Configuración de agente** de Consola de Cloud APM para inhabilitar o habilitar la recopilación de datos de diagnóstico en cualquier momento para uno o más sistemas gestionados.

Antes de empezar

- Debe tener instalado Cloud APM, Advanced en su entorno.
- Debe instalar y configurar Monitoring Agent for Ruby en una máquina virtual, tal como se describe en "Instalación de agentes" en la página 130 en sistemas AIX o "Instalación de agentes" en la página 138 en sistemas Linux y en "Configuración de la supervisión de Ruby" en la página 743.
- Debe instalar el recopilador de datos de diagnóstico y configurar el soporte para la recopilación de diagnósticos, como se describe en "Instalación del recopilador de datos" en la página 746.

Acerca de esta tarea

Tras configurar el soporte para los datos de diagnóstico en la configuración del recopilador de datos, la recopilación de datos de diagnóstico está inhabilitada de forma predeterminada para cada uno de los sistemas gestionados. Para visualizar datos en los paneles de instrumentos de diagnóstico, debe habilitar la recopilación de datos de diagnóstico para cada sistema gestionado que supervise.

Realice estos pasos para habilitar e inhabilitar la recopilación de datos de diagnóstico para cada sistema gestionado:

Procedimiento

1. En la barra de navegación, seleccione **Configuración del sistema->Configuración de agente**.
   Se mostrará la página **Configuración del agente**.
2. Pulse el separador **Ruby**.
3. Marque los recuadros de selección de los sistemas gestionados en los que desea inhabilitar o habilitar la recopilación de datos de diagnóstico.
4. En la lista **Acciones**, seleccione una de las opciones siguientes para inhabilitar o habilitar la recopilación de datos de diagnóstico para los sistemas gestionados seleccionados:
   - Seleccione **Inhabilitar recopilación de datos**. El estado de la columna `Recopilador de datos habilitado` se actualiza a `No` para cada uno de los sistemas gestionados seleccionados.
   - Seleccione **Habilitar recopilación de datos**. El estado de la columna `Recopilador de datos habilitado` se actualiza a `Sí` para cada uno de los sistemas gestionados seleccionados.

Resultados
Ha configurado la recopilación de datos de diagnóstico para cada uno de los sistemas gestionados seleccionados.

Configuración del Recopilador de datos de Ruby para aplicaciones de IBM Cloud

Para recopilar información sobre aplicaciones Ruby en IBM Cloud, debe configurar el Recopilador de datos de Ruby.

Antes de empezar

1. Descargue el paquete de recopilador de datos del sitio web de IBM Marketplace. Para obtener instrucciones detalladas, consulte "Descarga de los agentes y recopiladores de datos" en la página 107.

Procedimiento

1. Extraiga los archivos del paquete del recopilador de datos. El paquete `ruby_datacollector_8.1.4.0.tgz` está incluido en el directorio extraído.
2. Extraiga los archivos de `ruby_datacollector_8.1.4.0.tgz` ejecutando el mandato siguiente:

   ```
   tar -zxf ruby_datacollector_8.1.4.0.tgz
   ```

   Obtendrá una carpeta `ibm_ruby_dc`.
3. Copie toda la carpeta `etc` de `ibm_ruby_dc` en la carpeta raíz de la aplicación Ruby ejecutando el mandato siguiente:

   ```
   cp –r directorio a la carpeta etc  directorio de inicio de la aplicación Ruby
   ```

   El mandato siguiente extrae el recopilador de datos en el directorio `/opt/ibm/ccm/ibm_ruby_dc/etc` y el directorio de inicio de la aplicación Ruby es `/root/ruby_app/`:

   ```
   cp –r /opt/ibm/ccm/ibm_ruby_dc/etc /root/ruby_app/
   ```
4. Añada la sección siguiente a `Gemfile` en la carpeta de inicio de la aplicación Ruby:

   ```
   gem 'logger',  '>= 1.2.8'
   source 'https://maagemserver.ng.bluemix.net/' do
     gem 'ibm_resource_monitor'
     gem 'stacktracer'
   end
   ```
5. Ejecute el mandato `bundle lock` para volver a generar el archivo `Gemfile.lock`.
6. En el directorio que contiene el archivo `manifest.yml` de la aplicación Ruby ejecute el mandato siguiente:

   ```
   cf push
   ```

   Consejo: Para obtener un archivo `manifest.yml` de muestra, consulte "Ejemplo de archivo manifest.yml" en la página 196.

Resultados

El recopilador de datos se ha configurado y está conectado al Servidor de Cloud APM.

Qué hacer a continuación

Puede verificar que los datos de la aplicación IBM Cloud se visualizan en la Consola de Cloud APM. Para obtener instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte Inicio de la consola de Cloud APM. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte Gestión de aplicaciones.

Personalización del Recopilador de datos de Ruby para aplicaciones IBM Cloud

Puede añadir variables de entorno en la interfaz de usuario (IU) de IBM Cloudpara personalizar la supervisión de la aplicación IBM Cloud. Utilice la información siguiente para añadir las variables según sus necesidades.

Variables de entorno definidas por el usuario para el Recopilador de datos de Ruby

Puede utilizar la información de la tabla siguiente para personalizar la supervisión de Ruby en IBM Cloud.

Tabla 198. Variables de entorno definidas por el usuario soportadas para la supervisión de Ruby en IBM Cloud

Nombre de variable	Importancia	Valor	Descripción
APM_BM_GATEWAY_URL	Opcional	• https://*<ip o nombre de host del servidor>*:443 • http://*<ip o nombre de host del servidor>*:80	El URL de pasarela del servidor local de destino.
APM_KEYFILE_PSWD	Opcional	Contraseña cifrada del archivo de claves	La contraseña del archivo de claves cifrada que se empareja con el archivo de claves. Si es usuario de Linux, puede utilizar el mandato `echo -n <contraseña de archivo de claves> | base64` para cifrar la contraseña. **Nota:** establezca esta variable sólo cuando haya configurado la pasarela para utilizar HTTPS.
APM_KEYFILE_URL	Opcional	http://*<servidor http alojado>*:*<puerto>*/keyfile.p12	El URL utilizado para descargar el archivo de claves. **Nota:** establezca esta variable sólo cuando configure la pasarela para utilizar HTTPS.
kkm_instrumentation_enabled	Opcional	• verdadero • falso	Habilita o inhabilita la recopilación de datos de diagnóstico. true: si establece el valor en `true`, se recopilan datos de diagnóstico. False: si establece el valor en `false`, no se recopilan datos de diagnóstico. El valor predeterminado es `true`.

Tabla 198. Variables de entorno definidas por el usuario soportadas para la supervisión de Ruby en IBM Cloud (continuación)

Nombre de variable	Importancia	Valor	Descripción
kkm_max_methods_to_instrument	Opcional	Número máximo de métodos rastreados	El número máximo de métodos que se rastrean. Puede inhabilitar el rastreo de método estableciendo el valor en `0`. De forma predeterminada, el valor es `10000` y el método de rastreo está habilitado. **Nota:** es aconsejable no establecer un valor superior a 10000. Un valor muy superior a 10000 puede disminuir la eficiencia de ejecución de la aplicación.
kkm_sample_frequency	Opcional	Frecuencia de muestreo de solicitudes	El número de solicitudes a partir de cual se toma una solicitud de muestra, por ejemplo, si establece el valor en `10`, se recopilan datos de supervisión de una de cada 10 solicitudes. El valor predeterminado es `10`.
kkm_min_wallclock_to_include_in_trace	Opcional	Umbral de tiempo de respuesta para recopilar rastreo de método, en segundos	Si el tiempo de respuesta de una instancia de solicitud supera el valor de esta variable, el recopilador de datos recopila su rastreo de método. Por ejemplo, si se establece en 0,001, se rastrean las solicitudes y métodos cuyo tiempo de respuesta es superior a 1 milisegundo. El valor predeterminado es `0`, que significa que el rastreo de método está habilitado para todas las solicitudes y métodos.

Tabla 198. Variables de entorno definidas por el usuario soportadas para la supervisión de Ruby en IBM Cloud (continuación)

Nombre de variable	Importancia	Valor	Descripción
kkm_min_wallclock_to_include_stacks	Opcional	Umbral de tiempo de respuesta para recopilar el rastreo de pila, en segundos	Si el tiempo de respuesta de una instancia de solicitud excede el valor de esta variable, el recopilador de datos recopila su seguimiento de la pila. Por ejemplo, si se establece en 0,001, se rastrean las solicitudes y métodos cuyo tiempo de respuesta es superior a 1 milisegundo. El valor predeterminado es `0`, que significa que el rastreo de pila está habilitado para todas las solicitudes y métodos.

Desconfiguración del Recopilador de datos de Ruby para aplicaciones de IBM Cloud
Si no necesita supervisar el entorno de Ruby o si desea actualizar el Recopilador de datos de Ruby, primero debe desconfigurar varios valores del Recopilador de datos de Ruby.

Procedimiento

1. Vaya a la carpeta raíz de la aplicación.
2. Elimine las líneas siguientes de m`Gemfile` en la carpeta de inicio de la aplicación Ruby:

```
gem 'logger',  '>= 1.2.8'
source 'https://maagemserver.ng.bluemix.net/' do
  gem 'ibm_resource_monitor'
  gem 'stacktracer'
end
```

3. Ejecute el mandato `bundle lock`.
4. En el directorio de inicio de la aplicación, ejecute el mandato siguiente para volver a enviar la aplicación a IBM Cloud para que el cambio entre en vigor.

```
cf push
```

Resultados
Ha desconfigurado satisfactoriamente el Recopilador de datos de Ruby.

Qué hacer a continuación
Tras desconfigurar el recopilador de datos, la Consola de Cloud APM continúa mostrando el recopilador de datos en cualquier aplicación a la que haya añadido el recopilador de datos. La Consola de Cloud APM mostrará que no hay datos disponibles para la aplicación y no indicará que el recopilador de datos está fuera de línea. Para obtener información sobre cómo eliminar el recopilador de datos de aplicaciones y de grupos de recursos, consulte “Eliminación de recopiladores de datos de Consola de Cloud APM” en la página 196.

Configuración de la supervisión de SAP

Para supervisar un sistema SAP, el Monitoring Agent for SAP Applications debe conectarse a un servidor de aplicaciones en el sistema que se supervisará para que el agente pueda acceder al código ABAP (Advanced Business Application Programming) que se proporciona con el producto.

Antes de empezar

- Revise los requisitos previos de hardware y software, consulte Software Product Compatibility Reports para el agente de SAP
- El agente SAP no da soporte a sistemas SAP no Unicode.

Acerca de esta tarea

El Agente de SAP es un agente de varias instancias; debe crear la primera instancia e iniciar el agente de forma manual.

- Para configurar el agente en sistemas Windows, puede utilizar la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
  - "Configuración del agente en sistemas Windows" en la página 756
  - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 759
- Para configurar el agente en sistemas Linux o AIX, puede ejecutar el script y responder a las solicitudes, o utilizar el archivo de respuestas silencioso.
  - "Configuración del agente en sistemas Linux o AIX" en la página 758
  - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 759

Después de instalar el agente SAP, puede importar el transporte Advanced Business Application Programming (ABAP) en el sistema SAP para dar soporte a la recopilación de datos en el sistema SAP. Para obtener más información, consulte "Importación del transporte ABAP en el sistema SAP" en la página 763.

Después de configurar el agente SAP, debe verificar la configuración de agente. Para obtener más información, consulte "Verificación de la configuración del agente" en la página 771.

Después de configurar el agente SAP, puede añadir el número de Puerto de comunicaciones de base de datos necesario para la conformidad con OSLC (Open Source Lifecycle Collaboration). Para obtener más información, consulte "Adición de un número de Puerto de comunicaciones de base de datos" en la página 775.

Para suprimir el transporte ABAP del sistema SAP, debe importar el transporte de supresión al sistema SAP. Para obtener más información, consulte "Eliminación del transporte ABAP en el sistema SAP" en la página 770.

El nuevo diseño de CCMS está habilitado de forma predeterminado. La entrada está presente en la tabla de base de datos /IBMMON/ITM_CNGF para el parámetro isnewccmsdesign cuyo valor se establece en YES.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Configuración del agente en sistemas Windows

Puede configurar el Agente de SAP en sistemas Windows utilizando la ventana **IBM Performance Management** para que el agente pueda recopilar datos del servidor de aplicaciones SAP que se está supervisando.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Plantilla** bajo la columna **Tarea/Subsistema** y pulse **Configurar utilizando los valores predeterminados**.

   Se abrirá la ventana **Monitoring Agent for SAP Applications**.
3. En el campo **Especificar un nombre de instancia exclusivo**, escriba el nombre de una instancia del agente y pulse **Aceptar**.

   Importante: El nombre de la instancia de agente debe coincidir con el identificador de sistema de 3 dígitos (SID) del servidor de aplicaciones SAP gestionado. Por ejemplo, si el SID del servidor de aplicaciones SAP gestionado es PS1, especifique PS1 como nombre de instancia.
4. Configure el Agente de SAP en la modalidad de servidor de aplicaciones o la modalidad de grupo de inicio de sesión.
   - Complete los pasos siguientes para configurar el Agente de SAP en el modo de servidor de aplicaciones:
     a. En el campo **Modalidad de conexión**, seleccione **Modalidad de servidor de aplicaciones** y pulse **Siguiente**.
     b. En el área **Especificar información de servidor de aplicaciones**, especifique valores para los parámetros de configuración y pulse **Siguiente**.
     c. En el área **Especificar información de inicio de sesión del sistema SAP**, especifique valores para los parámetros de configuración y pulse **Aceptar**.

     Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 759
   - Complete los pasos siguientes para configurar el Agente de SAP en el modo de grupo de inicio de sesión:
     a. En el campo **Modalidad de conexión**, seleccione **Modalidad de grupo de inicio de sesión** y pulse **Siguiente**.
     b. En el área **Especificar información de grupo de inicio de sesión**, especifique valores para los parámetros de configuración y pulse **Siguiente**.
     c. En el área **Especificar información de inicio de sesión del sistema SAP**, especifique valores para los parámetros de configuración y pulse **Aceptar**.

     Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 759

   Importante: Para la modalidad de servidor de aplicaciones, es obligatorio configurar Dialog Instance con asignador en el sistema SAP donde está configurado el servidor de mensajes o ASCS. Para la modalidad de grupo de inicio de sesión, no es obligatorio configurar Dialog Instance con asignador en el sistema SAP donde está configurado el servidor de mensajes o ASCS.
5. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón la instancia de agente que ha creado y pulse **Iniciar**.

   Importante: Si desea crear otra instancia del Agente de SAP, repita los pasos 1 a 6. Utilice un identificador de sistema exclusivo para cada instancia del Agente de SAP que desee crear.

Qué hacer a continuación

- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.
- Debe editar la situación predefinida `R3_Alert_Crit` y la situación `R3_Alert_Warn` para establecer la condición del atributo de estado de alerta como `Alert Status!= DONE` para que estas situaciones no se desencadenen para las alertas CCMS cerradas.

Configuración del agente en sistemas Linux o AIX

Puede configurar el Agente de SAP en sistemas Linux o AIX para que el agente pueda recopilar datos del servidor de aplicaciones SAP que se está supervisando.

Procedimiento

1. En la línea de mandatos, cambie la vía de acceso al directorio de instalación de agente. Ejemplo: `/opt/ibm/apm/agent/bin`
2. Ejecute el mandato siguiente, donde nombre_instancia es el nombre que asignará a la instancia:

   `./sap-agent.sh config` *`nombre_instancia`*

   Importante: El nombre de la instancia de agente debe coincidir con el identificador de sistema de 3 dígitos (SID) del servidor de aplicaciones SAP gestionado. Por ejemplo, si el SID del servidor de aplicaciones SAP gestionado es PS1, especifique PS1 como nombre de instancia.
3. Cuando la línea de mandatos muestra el siguiente mensaje, escriba 1 y pulse Intro: `Edit 'Monitoring Agent for SAP Applications' setting? [1=Yes, 2=No]`
4. Configure el Agente de SAP utilizando la modalidad de servidor de aplicaciones o la modalidad de grupo de inicio de sesión.
   - Complete los pasos siguientes para configurar el Agente de SAP en el modo de servidor de aplicaciones:
     a. Cuando la línea de mandatos muestra el siguiente mensaje, escriba 1 y pulse Intro: `Connection Mode [ 1=Application Server Mode, 2=Logon Group Mode ]`
     b. Especifique valores para los parámetros de configuración.

     Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 759
   - Complete los pasos siguientes para configurar el Agente de SAP en el modo de grupo de inicio de sesión:
     a. Cuando la línea de mandatos muestra el siguiente mensaje, escriba 2 y pulse Intro: `Connection Mode [ 1=Application Server Mode, 2=Logon Group Mode ]`
     b. Especifique valores para los parámetros de configuración.

     Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 759

   Importante: Para la modalidad de servidor de aplicaciones, es obligatorio configurar Dialog Instance con asignador en el sistema SAP donde está configurado el servidor de mensajes o ASCS. Para la modalidad de grupo de inicio de sesión, no es obligatorio configurar Dialog Instance con asignador en el sistema SAP donde está configurado el servidor de mensajes o ASCS.
5. Ejecute el mandato siguiente para iniciar el Agente de SAP:

   `./sap-agent.sh start` *`nombre_instancia`*

   Importante: si desea crear otra instancia del Agente de SAP, repita los pasos 1 a 5. Utilice un identificador de sistema exclusivo para cada instancia del Agente de SAP que cree.

Qué hacer a continuación

- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.
- Debe editar la situación predefinida `R3_Alert_Crit` y la situación `R3_Alert_Warn` para establecer la condición del atributo de estado de alerta como `Alert Status!= DONE` para que estas situaciones no se desencadenen para las alertas CCMS cerradas.

Configuración del agente mediante el archivo de respuestas silencioso

Puede configurar el Agente de SAP en sistemas Windows, Linux o AIX utilizando el archivo de respuestas silencioso.

Procedimiento

1. En un editor de texto, abra el archivo `sap_silent_config.txt` que está disponible en la vía de acceso *dir_instalación*`\samples` y especifique valores para todos los parámetros de configuración.

   Windows `C:\IBM\APM\samples`

   Linux AIX `/opt/ibm/apm/agent/samples`

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 759
2. En la línea de mandatos, cambie la vía de acceso al directorio bin:

   Windows *dir_instalación*`\BIN`

   Linux AIX *dir_instalación*`\bin`
3. Ejecute el mandato siguiente:

   Windows `sap-agent.bat config` *nombre_instancia dir_instalación*`\samples\sap_silent_config.txt`

   Linux AIX `sap-agent.sh config` *nombre_instancia dir_instalación*`\samples\sap_silent_config.txt`

   Importante: El nombre de la instancia de agente debe coincidir con el identificador de sistema de 3 dígitos (SID) del servidor de aplicaciones SAP gestionado. Por ejemplo, si el SID del servidor de aplicaciones SAP gestionado es PS1, especifique PS1 como nombre de instancia.
4. Inicie el agente.

   Windows En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón la instancia de agente que ha creado y pulse **Iniciar**.

   Linux AIX Ejecute el mandato siguiente: `./sap-agent.sh start` *nombre_instancia*

   Importante: si desea crear otra instancia del Agente de SAP, repita los pasos 1 a 4. Utilice un identificador de sistema exclusivo para cada instancia del Agente de SAP que cree.

Qué hacer a continuación

- Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.
- Debe editar la situación predefinida `R3_Alert_Crit` y la situación `R3_Alert_Warn` para establecer la condición del atributo de estado de alerta como `Alert Status!= DONE` para que estas situaciones no se desencadenen para las alertas CCMS cerradas.

Parámetros de configuración del agente

Al configurar el Agente de SAP, puede cambiar el valor predeterminado de los parámetros, como el nombre de host de SAP y el número de sistema de SAP.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del Agente de SAP.

Tabla 199. Nombres y descripciones de los parámetros de configuración del Agente de SAP

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos
Nombre de host de SAP (primario)	El nombre de host del servidor de aplicaciones SAP al que se conecta el agente. Si los servidores SAP se comunican a través de una red LAN privada, los sistemas que alojan a los servidores tendrán dos o más tarjetas de red. Para el nombre de host, especifique un nombre por el que se pueda localizar el servidor de aplicaciones desde los sistemas externos, como por ejemplo, el inicio de sesión de SAPGUI. No utilice el nombre de host de LAN privada. El valor predeterminado es el nombre de host en el que se ha instalado el agente.	Sí	`saphost.domain.com`
Número de sistema SAP (primario)	El sistema SAP o número de instancia de dos dígitos que se utiliza para conectarse a un servidor de host de SAP. El valor predeterminado es 00.	Sí	
Nombre de host de SAP (alternativo 1)	La segunda opción para el nombre de host si el host primario no está disponible.	No	
Número de sistema SAP (alternativo 1)	Número de sistema del nombre de host del primero alternativo.	No	
Nombre de host de SAP (alternativo 2)	La tercera opción para el nombre de host si los hosts del nombre de host de SAP (primario) y del nombre de host de SAP (alternativo 1) no están disponibles.	No	
Número de sistema SAP (alternativo 2)	Número de sistema del nombre de host del segundo alternativo.	No	
Número de cliente de SAP	El número de cliente SAP para el inicio de sesión RFC en SAP. El valor predeterminado es 000. Si se utiliza el usuario predefinido de IBMMON_AGENT generado por ABAP, especifique el número de cliente que se ha especificado en la importación de transporte. Este número es el mismo que el número de cliente nnn bajo el perfil.	Sí	
ID de usuario de SAP	El ID de usuario SAP para el inicio de sesión RFC en SAP. El valor predeterminado es IBMMON_AGENT, que es el ID de usuario predefinido creado durante la importación.	Sí	
Contraseña de usuario de SAP	Utilice la contraseña predeterminada o especifique una contraseña diferente.	Sí	
Confirmar contraseña de usuario SAP	La contraseña que se especifica en el campo **Contraseña de usuario SAP**.	Sí	

Tabla 199. Nombres y descripciones de los parámetros de configuración del Agente de SAP (continuación)

Nombre de parámetro	Descripción	Campo obligatorio	Ejemplos
Código de idioma de SAP	El código de idioma que indica el idioma que utiliza el agente cuando se conecta al sistema SAP. El idioma especificado determina el idioma en el que se visualiza la información de SAP, como mensajes de alerta, mensajes de registro del sistema y mensajes de registro de trabajo. Todos los sistemas SAP se proporcionan en inglés y alemán. Si necesita otro idioma, confirme con su administrador de SAP que el idioma esté instalado en el sistema SAP. Si especifica un idioma que no está soportado, el agente no se puede conectar al sistema SAP. Se da soporte a los siguientes idiomas y códigos: • CS - Checo • EN - Inglés • FR - Francés • DE - Alemán • HU - Húngaro • IT - Italiano • ES - Español • JA - Japonés • KO - Coreano • PL - Polaco • PT - Portugués • RU - Ruso • ZH - Chino • ZF - Chino tradicional	Sí	
Rastreo de RFC	El valor de rastreo de RFC (Remote Function Call) para la variable *SAPTRACE*. Al seleccionar este recuadro de selección, activa el rastreo de RFC y el valor predeterminado es sin rastreo de RFC. Para la línea de mandatos, 2 = Sin rastreo y 1 = Rastrear. Dado que el rastreo de RFC genera amplia información de diagnóstico, utilícelo con precaución. Para obtener más información sobre el rastreo de RFC, póngase en contacto con el soporte de IBM.	No	
Grupo de inicio de sesión de SAP	El nombre del grupo de inicio de sesión del servidor SAP.	Sí	
Nombre de servidor de mensajes de SAP	El nombre de host del servidor de mensajes de SAP.	Sí	

Tabla 199. Nombres y descripciones de los parámetros de configuración del Agente de SAP (continuación)			
Nombre de parámetro	**Descripción**	**Campo obligatorio**	**Ejemplos**
Servicio de mensajes de SAP	El nombre del servicio en el que se encuentra el servidor de mensajes SAP. Debe incluir nombres de servicio en los siguientes archivos de servicios del sistema operativo: • `/etc/services` • `\windows\system32\drivers\etc \services`	Sí	Podría utilizar el nombre de servicio de mensajes sapmsTV1 o el número de puerto del servicio de mensajes completo 3601.
Cadena de direccionamiento de SAP	Especifique la cadena de direccionador de SAP si desea acceder al servidor SAP con un direccionador de SAP.	No	La serie de direccionador `/H/host/H/` debe estar en el formato siguiente: `/H/beagle/H/brittany/H/` o `/H/amsaix11.tivlab.raleigh.ibm.com/W/tivoli/H/amsaix25`
SNC	Especifique si desea habilitar o inhabilitar Secure Network Communications (SNC). El valor predeterminado es inhabilitado.	Sí	**sap_conn.sap_snc_mode** =`true` o `false`
Nivel de seguridad de SNC	El nivel de seguridad de SNC.	Sí	**sap_snc_mode1.sap_snc_qop**=*valor de QOP*. El valor predeterminado es 8.
Nombre SNC de cliente o agente	El nombre SNC del cliente o agente.	Sí	**sap_snc_mode1.sap_snc_client**= *Nombre SNC cliente*
Nombre SNC de socio o servidor SAP	El nombre SNC del socio o servidor SAP.	Sí	**sap_snc_mode1.sap_snc_server**= *Nombre SNC servidor*
Vía de acceso de biblioteca criptográfica de SAP	La vía de acceso de la biblioteca criptográfica de SAP.	Sí	**sap_snc_mode1.sap_snc_library**= *vía de acceso de biblioteca criptográfica*

El nombre de host de SAP se recorta según el límite de longitud de Nombre de sistema gestionado

El `Nombre de sistema gestionado` de los recursos que se publican en la consola de APM está limitado a 32 caracteres. El Agente de SAP admite el recorte del nombre de dominio para formar el `Nombre de sistema gestionado` dentro del límite.

Caso de ejemplo 1

El Nombre de sistema gestionado para el subnodo de tipo **Sys** tiene el formato siguiente:

SID-DBHOST:**Sys**
Donde:

- *SID* es el ID del sistema SAP.
- *DBHOST* es el nombre de host del sistema SAP.

Ejemplo:
Si *SID* es **P27** y *DBHOST* es **VPT02F90.mycorporation.co.in**, el nombre de dominio completo (FQDN) del Nombre de sistema gestionado que se forma será **P27-VPT02F90.mycorporation.co.in:Sys**.

Si el Nombre de sistema gestionado tiene más de 32 caracteres, el Agente de SAP lo recorta para formar el nombre de sistema gestionado **P27-VPT02F90:Sys**. El Nombre de sistema gestionado recortado del subnodo se publicará en la consola de APM.

Nota: Si la longitud del Nombre de sistema gestionado que incluye el nombre de dominio es inferior o igual a 32 caracteres, el FQDN del Nombre de sistema gestionado no se recortará. El FQDN del Nombre de sistema gestionado se publica en la consola de APM como corresponda.
El recorte del nombre de dominio, cuando es necesario para cumplir el límite de longitud de Nombre de sistema gestionado, es aplicable a todos los tipos de subnodo publicados por el Agente de SAP.

Caso de ejemplo 2

El Nombre de sistema gestionado para el subnodo de instancia de agente **mySAP** tiene el formato siguiente:

$SAPSYSTEMNAME-$dbhost:*$CTIRA_HOSTNAME*:**mySAP**
Donde:

- *$SAPSYSTEMNAME* es el nombre de instancia de agente especificado durante la configuración.
- *$dbhost* es el nombre de host del sistema SAP.
- *$CTIRA_HOSTNAME* es el nombre de host de la máquina del agente.

Ejemplo:
Si *$SAPSYSTEMNAME* es **SA2**, *$dbhost* es **VPT02F90.mycorporation.co** y *$CTIRA_HOSTNAME* es **mysap1-v27.mycorp.co**, el nombre de dominio completo (FQDN) del Nombre de sistema gestionado que se forma será **SA2-VPT02F90.mycorporation.co.in: mysap1-v27:mySAP**.

Nota: El nombre de dominio predeterminado del nombre de host de la máquina del agente se recorta y será **mysap1-v27**.

El Nombre de sistema gestionado tiene más de 32 caracteres. En primer lugar, el Agente de SAP recorta el nombre de dominio del nombre de host del sistema SAP para formar **SA2-VPT02F90 :mysap1-v27 :mySAP**.
Si el Nombre de sistema gestionado resultante sigue superando los 32 caracteres, el Agente de SAP recortará los caracteres finales del nombre de host de la máquina del agente para formar el Nombre de sistema gestionado dentro del límite de 32 caracteres. A continuación, el Nombre de sistema gestionado del subnodo se publicará en la consola de APM.

Importación del transporte ABAP en el sistema SAP

Puede instalar un Agente de SAP para cada sistema SAP en el que importa el transporte ABAP (Advanced Business Application Programming) para dar soporte a la recopilación de datos en el sistema SAP.

Antes de empezar

Antes de importar el transporte ABAP en el sistema SAP, asegúrese de que se cumplen los requisitos siguientes:

- Para importar la solicitud de transporte de producto, se necesita R3trans Versión 01.07.04, o posterior porque las tablas de exportación e importación de Dynpro son incompatibles. El funcionamiento básico

del agente no resulta afectado por los problemas de incompatibilidad entre Dynpro o las tablas de importación y exportación; sólo resultan afectadas las ventanas de configuración de SAP.

- Tiene que asegurarse de importar el transporte Agente de SAP V7.1.1 en el cliente donde esté disponible la configuración MAI para supervisar el sistema de Solution Manager. Para ver las características del sistema PI, importe el transporte Agente de SAP V7.1.1 en el sistema PI en un cliente donde esté disponible la configuración PI.
- Para ver datos en los widgets de grupo que están bajo el subnodo SLM, también de completar las configuraciones de MAI para PI y Solution Manager. También debe configurar la supervisión del proceso de negocio para que pueda ver datos en el widget de grupo Alertas de BPM. Para ver datos para el widget de grupo Alertas críticas y de prioridad alta más recientes, realice las tareas de configuración siguientes:
  - En Solution Manager 7.1, ejecute la transacción SOLMAN_SETUP y seleccione **Supervisión de Sistemas**, active o habilite el componente de terceros y añada **Implementación: Definición BADI para Reacciones de Alerta** y conector de terceros.
  - Establezca el filtro de ámbito en **Todas las alertas y métricas**.
  - Asegúrese de que el estado de Implementación es **Activo**.

  Para obtener más información, consulte las Notas de Online Service System (OSS), que incluyen una lista de los niveles de paquete de servicio de SAP necesarios:

  - Nota de OSS 454321
  - Nota de OSS 330267
  - Nota de OSS 743155
- Para supervisar los sistemas SAP, el Agente de SAP necesita los datos de estadísticas de SAP. En sistemas SAP 7.0, debe establecer el huso horario del sistema SAP para que coincida con el huso horario del sistema operativo de forma que las estadísticas de SAP se recopilen con las indicaciones de fecha y hora correctas. Del mismo modo, actualice el huso horario del sistema SAP para el Agente de SAP para que el agente pueda recopilar datos. Para obtener información adicional sobre este problema, consulte la Nota de SAP 926290.

Acerca de esta tarea
Para obtener información sobre la importación del transporte SAP, consulte "Importación del transporte SAP" en la página 766.

Requisitos relacionados con MAI Alert para importar el transporte de ABAP
Debe verificar los requisitos previos de MAI Alert antes de importar el transporte de ABAP.

Valores de configuración incluidos en el archivo `transport.prop`

Cuando utilice el nuevo mecanismo de captación de MAI Alert que incluye la captación de MAI Alerts sin configurar parámetros de notificación por correo electrónico y sin implementación de BAdi, tendrá que modificar el siguiente valor de configuración en el archivo `transport.prop`.

Añada la línea SPLEVEL=X, donde X es el nivel del paquete de soporte (SP) del sistema Solution Manager.

Por ejemplo, si el System ID es S10 y el nivel del paquete de soporte es 13, añada SPLEVEL=13.

Importante: para el sistema SAP con el nivel de SP 10 o posterior, el valor del atributo de nombre técnico (MEA) no se llena en el widget de grupo Alertas de MAI más recientes con calificación 'Roja' del panel de instrumentos de SAP Solution Manager cuando las alertas MAI se captan sin configurar la notificación por correo electrónico en SAP Solution Manager y sin la implementación de BAdi. El valor del atributo de nombre técnico (MEA) se llena en el widget de grupo Alertas de MAI más recientes con calificación 'Roja' del panel de instrumentos de SAP Solution Manager cuando las alertas MAI se captan configurando la notificación por correo electrónico en SAP Solution Manager y la implementación de BAdi.

Determinación del nivel antiguo y nuevo para obtener MAI Alerts en función del nivel del paquete (SP) de soporte de Solution Manager

Mecanismo de obtención de MAI Alert antiguo
Este mecanismo se basa en la configuración de valores de notificación por correo electrónico y la implementación de BAdi /IBMMON/ITM_IMPL_ALRTINBX con la interfaz IF_ALERT_DYN_COFIGURATION para recopilar alertas de MAI y enviarlas al Agente de SAP.

Mecanismo de obtención de MAI Alert nuevo
Este mecanismo se basa en la obtención de MAI Alerts sin configurar valores de notificación por correo electrónico y sin implementación de /IBMMON/ITM_IMPL_ALRTINBX BAdi con la interfaz IF_ALERT_DYN_COFIGURATION.

Puede utilizar la siguiente tabla para comprender la utilización del archivo `transport.prop` y su dependencia de la configuración de los valores de notificación por correo electrónico.

Tabla 200. Uso del archivo transport.prop y sus dependencias

Nivel SP del sistema SAP	**Valores de transport.prop**		**Configuración de los valores de notificación por correo electrónico**	**Mecanismo de MAI Alert que debe utilizarse**
	MAI_ CONFIGURED	**Nivel de SP de Solution Manager**		
Cualquiera	No o el archivo no existe	No aplicable	Configurado o no configurado	El subnodo SLM no aparece y se muestra el subnodo SOL en su lugar.
SP 6 a 9	Sí	Mencionado	Configurado	Mecanismo antiguo
SP 6 a 9	Sí	No mencionado	Configurado	Mecanismo antiguo
SP 6 a 9	Sí	No mencionado	No configurado	El mecanismo antiguo no funciona porque la configuración de los valores de notificación por correo electrónico es obligatoria.
SP 6 a 9	Sí	Mencionado	No configurado	El mecanismo antiguo no funciona porque la configuración de los valores de notificación por correo electrónico es obligatoria.
SP 10 o posterior	Sí	Mencionado	Configurado	Mecanismo nuevo
SP 10 o posterior	Sí	Mencionado	No configurado	Mecanismo nuevo
SP 10 o posterior	Sí	No mencionado	Configurado	Mecanismo antiguo

Tabla 200. Uso del archivo transport.prop y sus dependencias (continuación)				
Nivel SP del sistema SAP	**Valores de transport.prop**		**Configuración de los valores de notificación por correo electrónico**	**Mecanismo de MAI Alert que debe utilizarse**
	MAI_ CONFIGURED	**Nivel de SP de Solution Manager**		
SP 10 o posterior	Sí	No mencionado	No configurado	El mecanismo antiguo no funciona porque la configuración de los valores de notificación por correo electrónico es obligatoria.

Importación del transporte SAP
El Agente de SAP proporciona un conjunto de rutinas Advanced Business Application Programming (ABAP) para dar soporte a la recopilación de datos en el sistema SAP. Este código ABAP se proporciona como un transporte SAP que debe estar instalado en cada sistema SAP que se va a supervisar. El administrador SAP instala el transporte.

Acerca de esta tarea

El perfil de autorización **ZITM_610AUTH** y el rol de autorización **ZITM_610AUT** son válidos solo hasta el release 6.1. A partir del release 6.2, se utiliza el perfil de autorización **/IBMMON/AUTH**. Para protegerse frente al uso no autorizado, el código ABAP instalado en el sistema SAP no se puede ver desde el sistema SAP. Además, este código no se puede modificar ni generar. Debe obtener el soporte para este código del sitio web de soporte de software de IBM.

Además de instalar código ABAP, el transporte también instala elementos de texto de idioma traducido para proporcionar soporte multilingüístico para elementos de texto de transporte SAP.

Importante: Para importar el transporte en el sistema SAP, no debe iniciar la instancia del Agente de SAP configurada para supervisar el sistema SAP.

Al importar el transporte SAP, los usuarios se definen implícitamente en el sistema SAP.

Utilice este procedimiento para importar el transporte SAP en el sistema SAP.

Procedimiento

1. Copie el archivo de transporte de IBM Tivoli Monitoring de las vías de acceso siguientes del sistema en el que el agente está instalado.
   - Para Windows: *dir_instalación*\TMAITM6_x64\ABAP
   - Para no Windows: *dir_instalación*/*intrp*/sa/ABAP, donde *intrp* debe ser **lx8266** o **aix526**.
2. Copie los archivo de transporte siguientes de las vías de acceso mencionadas en el paso 1 en el entorno SAP:
   - K711_00xxxU.ITM y R711_00xxxU.ITM

     Estos archivos son versiones en Unicode del transporte. Contienen el código ABAP de Agente de SAP y soporte de Unicode para cadenas de texto de páginas de códigos de caracteres latinos y páginas de códigos de doble byte.
   - K711_00xxx_DELETE.ITM y R711_00xxx_DELETE.ITM

     Estos archivos eliminan el código ABAP. No es necesario importar el transporte DELETE, a menos que deje de utilizar el producto completamente y desee eliminar los transportes de los sistemas SAP. Consulte “Eliminación del transporte ABAP en el sistema SAP” en la página 770

3. Copie los archivos de transporte en el directorio de datos del sistema de transporte de SAP tal como se indica a continuación y no cambie el nombre del archivo de transporte:

   Transporte Unicode

   a. Copie el archivo K711_00xxxU.ITM en el directorio cofiles
   b. Copie el archivo R711_00xxxU.ITM en el directorio data.

4. Para instalar el único archivo de transporte de IBM Tivoli Monitoring en el sistema SAP, seleccione una de las siguientes opciones de importación de archivos:

   - Para el sistema SAP, con un nivel de Solution Manager 7.1 Service Pack 6, o posterior y con MAI configurado, debe crear el archivo transport.prop en el directorio de trabajo usr/sap/SID/DVEBMGS*instancenumber*/work del sistema SAP. Si el sistema SAP es un sistema distribuido con ABAP SAP Central Services (ASCS), cree el archivo transport.prop en el directorio usr/sap/SID de la Instancia central (CI). A continuación, añada la entrada MAI_CONFIGURED = YES en ese archivo. Esta entrada crea una entrada MAI_CONFIGURED = YES en la tabla /IBMMON/ITM_CNFG. Ahora puede importar el archivo de transporte único de IBM Tivoli Monitoring en el sistema SAP.

     Nota: Antes de importar el archivo de transporte único de IBM Tivoli Monitoring, debe crear el archivo transport.prop en el directorio de trabajo usr/sap/SID/DVEBMGS*instancenumber*/work del sistema SAP y añadir la entrada MAI_CONFIGURED = YES a ese archivo. No debe editar la entrada en la tabla /IBMMON/ITM_CNFG.
   - Para el resto de sistemas SAP que tienen una versión base igual a 7.0 o posterior y Solution Manager V7.1 sin configuración de MAI, debe importar directamente el archivo de transporte único de IBM Tivoli Monitoring.

5. Ejecute el siguiente mandato para importar el transporte SAP:

```
tp addtobuffer ITMK711_00xxxU SID
pf=\usr\sap\trans\bin\NOMBRE_PERFIL
```

   Donde:

   SID
   ID del sistema SAP de destino.

   NOMBRE_PERFIL
   Nombre del archivo de perfil de tp. Asegúrese de especificar el archivo de parámetros tp actual cuando importa los archivos de transporte de agente de la línea de mandatos. El archivo de parámetros tp se suele denominar TP_DOMAIN_*SID*.PFL. Este nombre de archivo distingue entre mayúsculas y minúsculas en sistemas UNIX.

   nnn
   Número del cliente de destino en el que se ejecuta el agente y para el que están definidos el ID de usuario, IBMMON_AGENT, el perfil de autorización y /IBMMON/AUTH.

   También puede utilizar la transacción SAP STMS para importar las solicitudes de transporte de ITMK711_00xxxU.ITM. Asegúrese de que las opciones siguientes están seleccionadas en la pestaña **Importar opciones** de la ventana **Importar solicitud de transporte**.

   - **Dejar solicitud de transporte en cola para importación posterior**
   - **Volver a importar solicitud de transporte**
   - **Sobrescribir originales**
   - **Sobrescribir objetos en reparaciones no confirmadas**

   Para la versión SAP Basis, si la opción **Ignorar versión de componente no válida** está habilitada, asegúrese de que está seleccionada.

Resultados
En función del nivel de release de SAP, al ejecutar el mandato **`tp import`** podría recibir un código de retorno 4, lo que no indica un problema. Recibir el código de retorno 4 es un resultado esperado del mandato **`import`**.

Usuarios y autorizaciones requeridos por Agente de SAP
Para proteger contra el acceso no autorizado al sistema SAP, puede asignar autorizaciones a un usuario que inicia la sesión en el sistema SAP. Estas autorizaciones definen los niveles de acceso para un usuario en el sistema SAP.

Después de importar el transporte ABAP, el agente SAP crea el ID de usuario predeterminado como IBMMON_AGENT en el sistema SAP con la contraseña predeterminada como ITMMYSAP. Este usuario es un usuario del sistema y el perfil de autorización /IBMMON/AUTH está asociado al usuario. El perfil / IBMMON/AUTH y el usuario IBMMON_AGENT se crean después de importar el transporte ABAP. Con el perfil /IBMMON/AUTH, el usuario IBMMON_AGENT puede acceder a transacciones que son necesarias para leer datos de rendimiento desde el sistema SAP. Algunos ejemplos de transacciones que se utilizan son los siguientes:

- Administración y alertas de CCMS
- Autorización para la supervisor de mensajes PI/XI
- Autorizaciones de Solution Manager

Puede crear cualquier otro usuario de tipo de sistema para el agente. Al usuario se le debe asignar el perfil /IBMMON/AUTH.

Para ver y acceder a datos de componentes SAP, asegúrese de que el usuario que se crea para el agente tiene todas las autorizaciones especificadas en la siguiente tabla:

Tabla 201. Lista de autorizaciones

Componentes	Objetos de autorización	Descripción de la autorización
La autorizaciones del sistema general que incluyen los siguientes componentes: • Instancia SAP • Sistema SAP	S_ADMI_FCD	Acceder al sistema SAP
	S_BDS_DS -BC-SRV-KPR-BDS	Acceder al conjunto de documentos
	S_BTCH_JOB	Ejecutar operaciones en los trabajos en segundo plano
	S_CCM_RECV	Transferir los datos de repositorio del sistema central
	S_C_FUNCT	Hacer llamadas a la función de kernel C en los programas ABAP
	S_DATASET	Acceder a archivos
	S_RFC	Comprobar el acceso RFC. El objeto de autorización de S_RFC contiene las dos subautorizaciones siguientes: • RFC1: para proporcionar las autorizaciones para el grupo de función RFC1. • SDIFRUNTIME: para proporcionar las autorizaciones para el grupo de función SDIFRUNTIME.
	S_RFCACL	Comprobar la autorización para usuarios RFC
	S_RZL_ADM	Acceder al Sistema de gestión de cambios de configuración (CCMS) para la administración del sistema R/3
	S_TCODE	Comprobar autorizaciones para iniciar las transacciones definidas para una aplicación
	S_TOOLS_EX	Visualizar registros de estadísticas externas en las herramientas de supervisión
Autorizaciones para PI que incluyen la integración de proceso de SAP	S_XMB_MONI	Acceder a la supervisión de mensajes XI

Tabla 201. Lista de autorizaciones (continuación)		
Componentes	**Objetos de autorización**	**Descripción de la autorización**
Autorizaciones para MAI que incluyen SAP Solution Manager	AI_DIAGE2E	Restringir funciones de diagnósticos de E2E
	AI_LMDB_OB	Acceder a objetos de LMBD (Landscape Management Database)
	SM_MOAL_TC	Controlar el acceso a la funcionalidad de alertas y supervisión en SAP Solution Manager
	SM_WC_VIEW	Restringir acceso a elementos de interfaz de usuario específicos en centros de trabajo de Solution Manager
	S_RFC_ADM	Controlar derechos para administrar destinos RFC
	S_RS_AUTH	Especificar autorizaciones de análisis dentro de un rol
	SM_APPTYPE	Acceder al tipo de app de Solution Manager
	SM_APP_ID	Acceder a aplicaciones proporcionadas en centros de trabajo

Eliminación del transporte ABAP en el sistema SAP

Si opta por eliminar Agente de SAP del sistema, debe importar el transporte 'delete' en el sistema SAP. El transporte Delete suprime los módulos de función y los objetos de diccionario del Agente de SAP.

Antes de empezar

Antes de suprimir el transporte del sistema SAP, deberá para la instancia del Agente de SAP configurada para supervisar el sistema SAP.

Si el sistema SAP está en la versión 7.20 o posterior, antes de importar el transporte delete, en el perfil de transporte, tiene que añadir el siguiente parámetro del perfil de transporte: **tadirdeletions=true**. Este parámetro del perfil de transporte está disponible en la versión de tp 375.57.68 y en R3trans versión 6.14, release 700, o posterior. Para obtener más información sobre cómo eliminar las solicitudes de transporte del sistema SAP, consulte Supresión de solicitudes de transporte.

Procedimiento

1. Vaya a la vía de acceso siguiente:
   - Para Windows: *dir_instalación*\TMAITM6_x64\ABAP
   - Para no Windows: *dir_instalación*/*intrp*/sa/ABAP, donde *intrp* debe ser **lx8266** o **aix526**.
2. Copie los archivos de transporte en el entorno SAP.
3. Copie los archivos K711_00xxx_DELETE y R711_00xxx_DELETE en el directorio de datos del Sistema de transporte de SAP de la forma siguiente:
   a) Copie el archivo K711_00xxx_DELETE en el directorio cofiles.
   b) Copie el archivo R711_00xxx_DELETE en el directorio data.

4. Ejecute los comandos siguientes para importar el transporte 'delete':
   a) **tp addtobuffer ITMK711_00xxx_DELETE SID pf=\usr\sap\trans\bin ***NOMBRE_PERFIL*
   b) **tp import ITMK711_00xxx_DELETE SID client=nnn U16 pf=\usr\sap\trans\bin** *NOMBRE_PERFIL*, donde:

      SID
      ID del sistema SAP de destino.

      NOMBRE_PERFIL
      Nombre del archivo de perfil de tp.

      nnn
      Número del cliente de destino en el que se debe ejecutar el agente.

Verificación de la configuración del agente

Después de instalar el Agente de SAP, debe verificar la configuración del agente descargando, copiando y verificando la biblioteca de NetWeaver RFC SDK V7.20. Debe verificar también la configuración de Solution Manager V7.1 con MAI_Monitoring, verificar las alertas MAI y verificar los valores de configuración específicos del componente de terceros.

Verifique la configuración del agente siguiendo estos procedimientos:

- "Descarga de la biblioteca de NetWeaver RFC SDK V7.20" en la página 771
- "Copia de la biblioteca de NetWeaver RFC SDK V7.20 en la configuración del agente SAP" en la página 772
- "Verificación de la biblioteca de NetWeaver RFC SDK V7.20" en la página 772
- "Verificación de la configuración de Solution Manager V7.1 con supervisión MAI" en la página 773
- "Verificación de alertas MAI" en la página 774
- "Verificación de valores de configuración específicos de componentes de terceros" en la página 774

Descarga de la biblioteca de NetWeaver RFC SDK V7.20

Descargar la biblioteca de NetWeaver RFC SDK V7.20 después de terminar de instalar el agente SAP. Todos los archivos relacionados con la biblioteca de NetWeaver RFC SDK V7.20 se pueden descargar del sitio web de SAP.

Procedimiento

1. Inicie la sesión en SAP Marketplace mediante el URL siguiente: http://service.sap.com
2. Pulse **SAP Support Portal**.
3. Especifique el nombre de usuario y la contraseña de Marketplace.
4. Pulse **Software Downloads** y expanda el enlace **Support Packages and Patches**.
5. Pulse **Browse our Download Catalog**, y a continuación pulse **Additional Components**.
6. Pulse **SAP NetWeaver RFC SDK** y a continuación pulse **SAP NetWeaver RFC SDK 7.20**.
7. Seleccione el sistema operativo en el que desea tener el agente SAP.
8. Descargue el archivo `*.SAR` en el sistema.
9. Para extraer el archivo SAP `Netweaver RFC SDK *.SAR` mediante el programa de utilidad SAPCAR proporcionado por SAP, ejecute el mandato siguiente:
   `sapcar -xvf` *`SAP NetWeaver RFC SDK File Name`*`.SAR`

   Nota: Puede descargar el programa de utilidad SAPCAR del sitio web de SAP.
10. Vaya a la carpeta `lib` dentro de la carpeta extraída.

Qué hacer a continuación

Copie la biblioteca de NetWeaver RFC SDK V7.20 en la configuración del agente SAP.

Copia de la biblioteca de NetWeaver RFC SDK V7.20 en la configuración del agente SAP
La biblioteca de NetWeaver RFC SDK V7.20 contiene archivos que debe copiar manualmente en la ubicación de configuración del agente SAP.

Procedimiento

1. Vaya al directorio en el que descargó la biblioteca de NetWeaver RFC SDK V7.20.
2. Copie los archivos en la ubicación de configuración del agente SAP.
   - En sistemas operativos Windows de 64 bits debe copiar los siguientes archivos:
     - `icuin34.dll`
     - `libicudecnumber.dll`
     - `libsapucum.dll`
     - `icudt34.dll`
     - `icuuc34.dll`
     - `sapnwrfc.dll`

     Debe copiar los archivos en la ubicación `install_dir\TMAITM6_x64`.
   - En sistemas operativos distintos de Windows, hay que copiar los archivos en la ubicación `dir_instalación/`*`intrp`*`/sa/lib`, donde *intrp* es el código del sistema operativo (aix526, li6263, sol606). Debe copiar los archivos siguientes:
     - `libsapnwrfc.so`
     - `ibicudecnumber.so`
     - `ibicuuc34.a`
     - `libicui18n34.a`
     - `libicudata34.a`
     - `libsapucum.so`

Qué hacer a continuación

Verifique la versión de la biblioteca de NetWeaver RFC SDK V7.20 que haya descargado.

Verificación de la biblioteca de NetWeaver RFC SDK V7.20
Debe verificar la versión del archivo después de copiar el archivos extraído.

Procedimiento

- Windows Para verificar la versión del archivo, complete los pasos siguientes:
  a) Pulse con el botón derecho sobre `sapnwrfc.dll` y pulse **Propiedades**.
  b) Pulse la pestaña **Versión**.
  c) En la sección **Versión del producto** asegúrese de tener la versión siguiente: 720, parche 514, lista de cambios 1448293 o posterior
- Linux AIX Para verificar la versión del archivo, complete los pasos siguientes:
  a) Vaya a la carpeta `lib` en el archivo `*.SAR` extraído.
  b) Ejecute el mandato siguiente **`strings libsapnwrfc.so | grep SAPFileVersion`**
  c) Debe ver el mensaje siguiente `[root@IBMSAP2V6 lib]# strings libsapnwrfc.so | grep SAPFileVersion GetSAPFileVersion #[%]SAPFileVersion: 7200, 514, 22, 6206 .GetSAPFileVersion`

  Nota: El mensaje muestra que esta biblioteca tiene la versión 720 parche 514 o posterior.

Verificación de la configuración de Solution Manager V7.1 con supervisión MAI

Para recibir datos para Alertas MAI debe verificar si Solution Manager V7.1 está correctamente configurado.

Acerca de esta tarea

Puede utilizar Solution Manager V7.1 con supervisión de MAI e infraestructura de alertas para supervisar los sistemas gestionados. Solution Manager V7.1 se supervisa a sí mismo y a los sistemas satélite. Cada sistema de satélite tiene un plug-in y agentes de diagnóstico. Los agentes de diagnóstico captan los datos para el nivel de host o de sistema operativo. Cada host puede tener varios agentes de diagnóstico para diferentes Solution Managers que supervisen el host. A continuación se proporcionan las palabras clave utilizadas en la supervisión de MAI de Solution Manager:

- Medidas: datos de los sistemas satélite.
- Alertas: notificaciones basadas en el traspaso de algunos valores de umbral que se pueden configurar.
- Incidente: alertas convertidas en incidencias y asignadas a cualquier usuario.

Para verificar la configuración de Solution Manager V7.1 con MAI debe verificar los valores básicos, los valores de nivel global y los valores de nivel de plantilla.

Procedimiento

1. Para verificar los valores básicos, especifique el código de transacción SOLMAN_SETUP y pulse **Intro**.
   Asegúrese de que todos los LEDs están en verde en los separadores siguientes:
   - Visión general
   - Configuración básica
   - Configuración del sistema gestionado

   Nota: Hay categorías diferentes de sistemas gestionados, como por ejemplo sistemas técnicos, casos prácticos técnicos, host, base de datos, instancia, dominio de PI, componente técnico y conexión. Debe configurar estos sistemas gestionados según los requisitos empresariales. Las alertas MAI están basadas en los sistemas gestionados configurados.
2. Especifique el código de transacción: SE38 y pulse **Intro**.
3. Proporcione el nombre del programa como RTCCTOOL y ejecute el informe.
   Asegúrese de que todos los LEDs están en verde en la salida.
4. Para verificar los valores de nivel global, especifique el código de transacción: SOLMAN_WORKCENTER y pulse **Intro**.
   Asegúrese de que todos los LEDs están en verde en los separadores siguientes:
   - Visión general
   - Configurar infraestructura
   - Requisitos previos
   - Configurar
5. Verifique si el estado de **Valores globales** para **Notificación** es **Activo**.
6. Para verificar los valores de nivel de plantilla, especifique el código de transacción SOLMAN_SETUP y pulse **Intro**.
   En **Valores técnicos**, en la lista **Notificaciones automáticas**, asegúrese de **Activo** está seleccionado.

   Nota: A efectos de resolución de problemas iniciales, asegúrese de que las notificaciones de correo electrónico estén activas.
7. A efectos de la supervisión del sistema MAI, verifique la configuración de End-User Experience Monitoring (EEM) siguiendo estos pasos:
   a) Especifique el código de transacción SE37 y pulse **Intro**.
   b) Especifique **AI_EEM_LIST_ALL_SCENARIOS** en el campo **Nombre de módulo de función** y pulse F8.

Debe haber una entrada para End-User Experience Monitoring (EEM).

Verificación de alertas MAI
Para asegurarse de que MAI de Solution Manager está correctamente configurado para supervisar la Entrada de alertas MAI en la Supervisión técnica, debe verificar que recibe Alertas MAI como salida.

Procedimiento

1. Especifique el código de transacción SOLMAN_WORKCENTER y pulse **Intro**. Compruebe si puede ver Alertas de MAI en el Buzón de alertas de MAI de Solution Manager, bajo Supervisión técnica.
2. Compruebe la implementación de BAdi siguiendo estos pasos:
   a) Especifique el código de transacción SE19 y pulse **Intro**
   b) Especifique /IBMMON/ITM_IMPL_ALRTINBX en el campo **Implementación de mejora**.
   c) Pulse **Visualizar** y compruebe si la implementación BAdi está activa en la sección **Comportamiento de tiempo de ejecución**.
3. Compruebe si la base de datos /IBMMON/ITM_ALIX contiene Alertas de MAI siguiendo estos pasos:
   a) Especifique el código de transacción SE16 y pulse **Intro**.
   b) En el campo **Nombre de tabla**, especifique /IBMMON/ITM_ALIX y ejecútela. Asegúrese de recibir Alertas MAI en la tabla.
4. Especifique el código de transacción: SE37 y pulse **Intro**.
5. En el campo **Nombre de módulo de función**, especifique /IBMMON/ITM_MAIALRT_INX y pulse F8.
   Debe ver Alertas MAI como salida.

Qué hacer a continuación
Si no puede ver Alertas MAI en la base de datos IBMMON/ITM_ALIX, debe verificar los valores del componente de terceros.

Verificación de valores de configuración específicos de componentes de terceros
Si no puede ver alertas MAI, deberá verificar los valores del componente de terceros.

Procedimiento

1. Verifique que el componente de terceros está activo.
2. Verifique que en **Adaptador de sistema operativo**, bajo **Implementación BAdi**, **Reacción de alerta** está disponible. Si **Reacción de alerta** no está disponible, elimine los valores predeterminados y seleccione **Implementación BAdi - Reacción de alerta**.
3. Compruebe los valores de plantilla mediante los pasos siguientes:
   a) Verifique los valores que se utilizan para transferir alertas específicas al sistema de terceros, como por ejemplo SAP ABAP 7.0.0.
   b) Seleccione **Modalidad experta**, seleccione **Alertas** y pulse **Componente de terceros**.
   Asegúrese de que puede ver el nombre BAdi de reacción de alerta.

   Nota: Asegúrese de que las últimas notas de SAP estén implementadas. Para Solution Manager V7.1 Service Pack 8, compruebe si las notas siguientes están implementadas:

   - https://service.sap.com/sap/support/notes/1959978
   - https://service.sap.com/sap/support/notes/1820727
4. Si no puede ver Alertas de MAI en la base de datos /IBMMON/ITM_MAIALRT_INX, debe seguir estos pasos de configuración de MAI de Solution Manager para el componente de terceros:
   a) Especifique el código de transacción SOLMAN_SETUP y pulse **Intro**.
   b) En **Supervisión técnica**, seleccione **Supervisión de sistema**.
   c) Pulse el separador **Configurar infraestructura** y a continuación pulse el separador **Valores predeterminados**.

d) Pulse el separador **Componentes de terceros** y a continuación pulse **Editar**.

e) Seleccione **Activo** de la lista.

f) Asegúrese de que el filtro de ámbito está establecido como **Todas las alertas, sucesos y medidas (con sucesos internos)** para el conector seleccionado.

Nota: El Adaptador de mandatos del sistema operativo también es uno de los métodos para enviar datos al conector de terceros. Para configurar el Adaptador de mandatos del sistema operativo, consulte detalles de configuración en la guía de utilización del Adaptadores de mandatos del sistema operativo.

Adición de un número de Puerto de comunicaciones de base de datos

Es necesario tener un número de Puerto de comunicaciones de base de datos para identificar exclusivamente la entidad de base de datos en los escenarios integrados. Para conseguir una colaboración entre componentes, los componentes de SCM AI incluyen OSLC (Open Source Lifecycle Collaboration). En la conformidad de OSLC es esencial identificar exclusivamente los componentes colaboradores. Por lo tanto, es importante el número de Puerto de comunicaciones de base de datos.

Acerca de esta tarea

Al importar el transporte relevante de IBM Tivoli Monitoring al sistema SAP, la tabla de la base de datos `/IBMMON/ITM_PORT` se crea automáticamente. La tabla contiene los campos de base de datos siguientes:

- ID del sistema
- Nombre de host del sistema
- Número de Puerto de comunicaciones de base de datos

Procedimiento

Para añadir un número de Puerto de comunicaciones de base de datos de SAP para el Agente de SAP necesario para la conformidad de OSLC, siga estos pasos:

1. Vaya al Código de transacción SE16 y pulse Intro.
2. En el campo **Nombre de tabla de base de datos**, especifique `/IBMMON/ITM_PORT`y pulse F7.
3. Cuando aparezca la pantalla de selección de la tabla de base de datos de **/IBMMON/ITM_PORT**, pulse F8.

   La tabla de base de datos **/IBMMON/ITM_PORT** contiene los tres campos de base de datos siguientes:

   - ID del sistema
   - Nombre de host del sistema
   - Número de Puerto de comunicaciones de base de datos

   Nota: Los sistemas SAP que aparecen en la tabla de la base de datos `/IBMMON/ITM_PORT` son para ambas arquitecturas, Java y ABAP.
4. En el campo **Número de Puerto de comunicaciones de base de datos**, especifique el número de Puerto de comunicaciones de base de datos de SAP relevante para los respectivos ID del sistema SAP y nombre de host del sistema SAP y guarde los cambios.

   Nota: Si no especifica ningún valor en el campo **Número de puerto de comunicaciones de base de datos** en la tabla de base de datos `/IBMMON/ITM_PORT`, de forma predeterminada, el número de Puerto de comunicaciones de base de datos será 0.

Instalación y configuración avanzada del agente SAP

Se trata de instalaciones y configuraciones avanzadas que son específicas de Agente de SAP.

Se describen los siguientes temas de instalación y configuración:

- “Módulo de función SAP” en la página 776

- "ID de usuario de SAP" en la página 777
- Programas de utilidad del Agente de SAP
- "Conexiones RFC de SAP" en la página 777
- "Característica Probar conexión" en la página 788
- "Configuración avanzada opcional en SAP" en la página 780
- "Creación de informes del CCMS centralizado" en la página 786
- "Desinstalación del transporte ABAP (Advanced Business Application Programming) del sistema SAP" en la página 788

Nota: La instalación y configuración avanzada del Agente de SAP contiene referencias a IBM Tivoli Monitoring para que la documentación sea compatible con la interfaz de usuario del código de transacción personalizado del transporte ABAP.

Módulo de función SAP
Cuando el volumen de datos es alto en el servidor SAP, es posible que experimente problemas con ciertos widgets que causan un tiempo de respuesta lento del servidor. Si los widgets no son críticos, puede inhabilitar el módulo de función SAP asociado.

De forma predeterminada, los módulos de función de Agente de SAP están habilitados. Sin embargo, los siguientes módulos de función están inhabilitados de forma predeterminada:

- Servicios HTTP en el subnodo SYS (`/IBMMON/ITM_HTTP_SRVS`)
- Mensajes XML en el subnodo PI/XI (`/IBMMON/ITM_SXMB_MONI_NEW`)
- Comunicación síncrona/asíncrona en el subnodo PI/XI (`/IBMMON/ITM_SYN_ASYN_COMM`)
- Detalles de cola entrante qRFC en el subnodo Sys (`/IBMMON/ITM_QIN_QDETAILS`)

Después de inhabilitar el módulo de función SAP, si selecciona un widget, los datos no se visualizan en el panel de instrumentos de IBM Application Performance Management. Por lo tanto, se evitan los problemas relacionados con el rendimiento.

Habilitación del módulo de función del agente SAP
Si anteriormente ha inhabilitado el módulo de función de Agente de SAP para resolver los problemas de rendimiento, puede habilitar también el módulo de función.

Procedimiento

1. Inicie la sesión en el sistema SAP.
2. Ejecute el código de transacción SE16.
3. Especifique el nombre de la tabla como `/IBMMON/ITM_CNFG`.
4. Seleccione la fila que desea suprimir y pulse **Mayús + F2** para suprimir la entrada.
5. Pulse **Guardar**.

Inhabilitación del módulo de función SAP
Algunos widgets pueden provocar una respuesta lenta del servidor SAP, por lo que puede inhabilitar el módulo de funciones SAP para mejorar el rendimiento del servidor.

Procedimiento

1. Inicie la sesión en el sistema SAP.
2. Ejecute el código de transacción SE16.
3. Especifique el nombre de la tabla como `/IBMMON/ITM_CNFG`.
4. Pulse **F5** para crear una nueva entrada.
5. Escriba el nombre del módulo de función SAP en el campo **PARM NAME**.
6. Escriba No en el campo **VALUE CHAR**.
7. Pulse **Guardar**.

ID de usuario de SAP
En esta sección se proporciona información sobre los ID de usuario de SAP y los permisos que requiere Agente de SAP.

Los ID de usuario dan soporte a los fines siguientes:

- "Conexiones RFC de SAP" en la página 777
- "Supervisión básica del agente" en la página 777

Conexiones RFC de SAP
El Agente de SAP utiliza conexiones de llamadas a función remotas (RFC) para el sondeo interno de Centralized Computing Center Management (CCMS) y la recopilación de datos de alertas de CCMS. Este comportamiento es específico de la arquitectura RFC de SAP.

El Agente de SAP abre una conexión RFC dedicada en el sistema SAP que el agente supervisa. A continuación, el sistema SAP abre una conexión interna por servidor de aplicaciones para la recopilación de datos mediante programas y módulos de función. Si el agente recopila las alertas del CCMS, el sistema SAP abre una conexión RFC adicional (interna del sistema) con cada servidor de aplicaciones para esta hebra de recopilación. Cuando se inicia la recopilación de datos, se abre una conexión RFC para el agente. A continuación, se abren hasta el doble de servidores de aplicaciones SAP para conexiones RFC adicionales internas del sistema.

Debe asegurarse de que la instancia que supervisa puede acomodar las sesiones RFC adicionales, especialmente en sistemas grandes con 10 instancias o más. Si la carga anticipada de RFC para la supervisión puede afectar negativamente a las tolerancias y el rendimiento del sistema, ajuste el parámetro de perfil SAP. Póngase en contacto con el administrador de SAP y consulte las siguientes notas de SAP:

- Sesiones de terminal (valor predeterminado: 200) 22099
- Valores de comunicacón/pasarela/conversación 887909 316877 384971

Supervisión básica del agente
El Agente de SAP crea un IBMMON_AGENT en el sistema SAP cuando se importa el transporte del agente.

Este ID de usuario es IBMMON_AGENT, con la contraseña predeterminada ITMMYSAP. Está preconfigurado para que sea de tipo de comunicación de solo usuario y para utilizar el perfil de autorización /IBMMON/AUTH. Este perfil, que se crea durante la importación del transporte, contiene el conjunto mínimo de permisos para ejecutar el código ABAP (Advanced Business Application Programming) del agente. Además, este perfil acepta un conjunto de acciones limitadas en el sistema SAP.

Si este nombre de ID de usuario es inaceptable, por ejemplo, si infringe los convenios de denominación de la instalación, puede crear un ID de usuario diferente. El ID de usuario puede ser cualquier ID de usuario de SAP permitido, pero requiere el conjunto completo de permisos en el perfil /IBMMON/AUTH. EL ID de usuario requiere el acceso de tipo de comunicación de solo usuario.

El ID de usuario predeterminado proporciona suficiente autoridad solo para estos objetivos:

- Supervisar y recopilar datos
- Cerrar alertas de Computing Center Management System (CCMS)
- Habilitar, inhabilitar y restablecer estadísticas de pasarela
- Restablecer estadísticas de base de datos de Oracle

Si opta por limitar las prestaciones de acción del agente, puede eliminar algunos de los permisos de acción como por ejemplo cerrar alertas CCMS.

Para acceder a datos en el portal de la interfaz de usuario de IBM Application Performance Management para componentes específicos, asegúrese de tener las autorizaciones adecuadas. En la tabla siguiente se listan las autorizaciones necesarias para acceder a los datos de distintos subnodos:

Tabla 202. Lista de autorizaciones		
Subnodos	**Objetos de autorización**	**Descripción de la autorización**
Autorizaciones generales del sistema que incluyen los siguientes subnodos: • Ins • Sys	S_ADMI_FCD	Para acceder al sistema
	S_BDS_DS -BC-SRV-KPR-BDS	Para acceder al conjunto de documentos
	S_BTCH_JOB	Para ejecutar operaciones en los trabajos en segundo plano
	S_CCM_RECV	Para transferir datos del repositorio central del sistema
	S_C_FUNCT	Para realizar llamadas C en programas ABAP
	S_DATASET	Para acceder a archivos
	S_RFC	Para comprobar el acceso RFC. El objeto de autorización de S_RFC contiene las dos subautorizaciones siguientes: • RFC1: para proporcionar las autorizaciones para el grupo de función RFC1. • SDIFRUNTIME: para proporcionar las autorizaciones para el grupo de función SDIFRUNTIME.
	S_RFCACL	Para el usuario RFC
	S_RZL_ADM	Para acceder a Computing Center Management System (CCMS): Administración del sistema
	S_TCODE	Para comprobar el código de transacción al inicio de la transacción
	S_TOOLS_EX	Para acceder al supervisor de rendimiento de las herramientas

Tabla 202. Lista de autorizaciones (continuación)

Subnodos	Objetos de autorización	Descripción de la autorización
Autorizaciones para Solution Manager que incluyen los subnodos siguientes: • Lds • Sol	D_MD_DATA -DMD	Para ver contenido de datos de datos maestros
	D_SOLMANBU	Para acceder a un tipo de sesión de Solution Manager
	D_SOLM_ACT	Para acceder a una solución en Solution Manager
	D_SOL_VSBL	Para visualizar una solución en Solution Manager
	S_CTS_SADM	Para ver administración específica del sistema (transporte)
	S_TABU_RFC	Para ver comparación de cliente y copia: exportación de datos con RFC
Autorizaciones para PI que incluyen el subnodo PI	S_XMB_MONI	Para acceder a la supervisión de mensajes XI
Autorizaciones para MAI que incluyen el subnodo SLM	AI_DIAGE2E	Para acceder al análisis integral de Solution Diagnostics
	AI_LMDB_OB	Para acceder a objetos LMDB (Landscape Management Database)
	SM_MOAL_TC	Para acceder a Supervisión y alertas
	SM_WC_VIEW	Para acceder a elementos de la interfaz de usuario del centro de trabajo
	S_RFC_ADM	Para acceder a las opciones de administración para el destino RFC
	S_RS_AUTH	Para acceder a Análisis BI en rol
	SM_APPTYPE	Para acceder al tipo de aplicación de Solution Manager
	SM_APP_ID	Para acceder a las aplicaciones proporcionadas en el centro de trabajo

Utilización de Central User Administration (CUA)
Central User Administration (CUA) se utiliza para supervisar un sistema SAP.

Procedimiento

Para utilizar el rol de autorización e ID de usuario predefinidos para supervisar un sistema SAP configurado con Central User Administration, realice uno de los pasos siguientes:

- Instale el transporte en el cliente de sistema lógico padre de Central User Administration.

- Cree manualmente el ID de usuario o rol en el cliente donde desea instalar el transporte. El ID de usuario o rol está en el cliente donde se ha instalado (importado) el transporte.
- Cree manualmente el ID de usuario o rol en el cliente de sistema lógico padre de Central User Administration. A continuación, distribuya el ID de usuario o rol al cliente donde se ejecuta el agente.
- Cree manualmente el ID de usuario o rol en el cliente de sistema lógico padre de Central User Administration y ejecute el agente en este cliente.

Configuración avanzada opcional en SAP
Puede configurar el Agente de SAP utilizando las funciones SAP proporcionadas por agente o SAP estándar.

Utilice las transacciones proporcionadas por el agente en SAP para personalizar diversos comportamientos del agente. Después de ejecutar la transacción `/n/IBMMON/ITM_CONFIG` para acceder al menú de configuración principal en SAP, seleccione una de las opciones de configuración siguientes:

- "Característica de copia, copia de seguridad y restauración y transacciones" en la página 780
- "Copiar, hacer copia de seguridad y restaurar datos mediante transacciones" en la página 781
- "Herramienta de programa de utilidad de línea de mandatos" en la página 782
- "Ejecución del programa de utilidad de línea de mandatos en un entorno Windows " en la página 782
- "Ejecución del programa de utilidad de línea de mandatos en un entorno no Windows" en la página 783
- "Mantenimiento de alertas" en la página 783
- "Transacción Seleccionar conjuntos de supervisores y supervisores" en la página 784
- "Configurar umbral de respuesta de paso del diálogo en el sistema SAP" en la página 785

Nota: Debe anteponer `/n` como prefijo a todas las transacciones `/IBMMON/ITM*`.

El Agente de SAP utiliza inmediatamente los cambios de configuración realizados en estas transacciones, con la excepción de aquellos cambios que se han realizado para mantener los grupos gestionados. Cuando la configuración de los grupos gestionados cambia, el Agente de SAP descubrirá los cambios en el siguiente latido.

Utilice las funciones estándar de SAP para completar la siguiente configuración: "Configurar umbral de respuesta de paso del diálogo en el sistema SAP" en la página 785

Característica de copia, copia de seguridad y restauración y transacciones
Las características de copia, copia de seguridad y restauración están disponibles después de iniciar la sesión en el servidor SAP y ejecutar la transacción siguiente: `/n/IBMMON/ITM_CONFIG`.

Las operaciones de copia, copia de seguridad y restauración le permiten copiar, realizar copias de seguridad y restaurar los datos de configuración de IBM Tivoli Monitoring.

Utilice esta característica para seleccionar de entre las siguientes funciones y guardar los datos de configuración de IBM Tivoli Monitoring:

- **Copiar**

  Utilice esta característica para copiar los valores de configuración de IBM Tivoli Monitoring de un servidor SAP a otro servidor SAP. Por ejemplo, es posible que desee copiar los valores de configuración de IBM Tivoli Monitoring del agente **a1** a la instancia de servidor SAP SAP2. Este agente se ejecuta en el sistema **m1** y se configura para la instancia de servidor SAP 1 de SAP. Todos los valores de configuración de IBM Tivoli Monitoring, excepto los valores de supervisión de la instancia de servidor SAP, se copian en el sistema SAP de destino. Puede implementar la característica de copia mediante el programa de utilidad de línea de mandatos o la interfaz gráfica de usuario de SAP.
- **Copia de seguridad**

  Puede almacenar configuraciones específicas de agentes que ha completado en el servidor SAP realizando una copia de seguridad del sistema. Utilice esta característica para guardar los valores de configuración específicos de IBM Tivoli Monitoring en el sistema SAP. Puede utilizar la transacción /

IBMMON/ITM_CONFIG para especificar los valores. El archivo de copia de seguridad se almacena en el directorio de trabajo en el servidor SAP en la siguiente vía de acceso: /usr/sap//DVEBMGS/work.

- **Restaurar**

  Utilice esta característica para restaurar los datos de configuración de IBM Tivoli Monitoring en el servidor SAP desde el directorio de trabajo. Puede restaurar los datos de configuración de IBM Tivoli Monitoring en el mismo servidor SAP donde ha completado el procedimiento de copia de seguridad de estos datos de configuración u otro servidor SAP. Puede restaurar los datos de configuración de IBM Tivoli Monitoring en tablas específicas de SAP y de IBM Tivoli Monitoring. Los archivos de configuración se almacenan con una indicación de fecha y hora para que pueda seleccionar el punto en el que quiere restaurar sus archivos.

Las configuraciones específicas del agente incluyen valores de configuración en la transacción /IBMMON/ITM_CONFIG en SAP. Puede completar los siguientes procedimientos de configuración:

- Muestrear la frecuencia de las alertas.
- Habilitar alertas específicas.
- Almacenar nombres de archivo de registro.
- Gestionar definiciones de grupo.
- Seleccionar conjuntos de supervisores y supervisores.
- Seleccionar instancias de SAP para fines de supervisión.

Copiar, hacer copia de seguridad y restaurar datos mediante transacciones
En la interfaz de usuario de SAP puede copiar, hacer copia de seguridad y restaurar datos mediante la transacción /n/IBMMON/ITM_CONFIG.

Antes de empezar
Utilice los procedimientos de copia, copia de seguridad y restauración para copiar los valores de configuración de IBM Tivoli Monitoring de un servidor SAP en otro servidor SAP. Todos los valores de configuración de IBM Tivoli Monitoring, excepto los valores de supervisión de la instancia del servidor SAP, se copian en el sistema SAP de destino.

Procedimiento

Complete los siguientes procedimientos para copiar, hacer copia de seguridad y restaurar los datos en SAP:

- **Copiar**
  a. Especifique el ID del sistema SAP de destino y el nombre de archivo existente como `id de sistema de origen__<nombre de archivo>fecha_hora`.

     La transacción /IBMMON/ITM_COPY crea un archivo de configuración de IBM Tivoli Monitoring en el directorio de trabajo con el nombre de archivo `ID de sistema SAP de destino SAP__<nombre_archivo>_fecha_hora`.
  b. Pulse **Ejecutar** para copiar los datos de configuración de IBM Tivoli Monitoring en el archivo.
  c. Pulse **Atrás** o **Cancelar** para volver a la pantalla de configuración de IBM Tivoli Monitoring anterior.

     Los parámetros de entrada esperados son **`ID de sistema de destino`** y **`nombre_archivo`** que se van a copiar.
- **Copia de seguridad**
  a. Inicie la sesión en el servidor SAP e inicie la transacción /IBMMON/ITM_CONFIG.
  b. Seleccione **Copia de seguridad**.
  c. Especifique el nombre de archivo de copia de seguridad.

     El nombre de archivo se almacena como `sys_id_<nombre_archivo>_fecha_hora`.

d. Pulse **Ejecutar** para ejecutar la copia de seguridad y almacenar el archivo en el servidor de aplicaciones.

Nota: El archivo de copia de seguridad se almacena en el directorio de trabajo del servidor de aplicaciones.

e. Pulse **Atrás** o **Cancelar** para volver a la pantalla de configuración de IBM Tivoli Monitoring anterior.

- **Restaurar**

a. Inicie la sesión en el servidor SAP e inicie la transacción `/IBMMON/ITM_CONFIG`.

b. Seleccione **Restaurar**.

c. Escriba el nombre de archivo que se debe restaurar como `sys_id_<nombre_archivo>_fecha_hora`.

d. Pulse **Ejecutar** para restaurar los datos de configuración de IBM Tivoli Monitoring.

e. Pulse **Atrás** o **Cancelar** para volver a la pantalla de configuración de IBM Tivoli Monitoring anterior.

Herramienta de programa de utilidad de línea de mandatos

Puede utilizar la herramienta de programa de utilidad de línea de mandatos para copiar, realizar copias de seguridad y restaurar datos de configuración de IBM Tivoli Monitoring en el servidor SAP.

Puede ejecutar la herramienta de programa de utilidad de línea de mandatos en entornos Windows y no Windows. Consulte "Ejecución del programa de utilidad de línea de mandatos en un entorno Windows " en la página 782 y "Ejecución del programa de utilidad de línea de mandatos en un entorno no Windows" en la página 783.

- **Copiar**

  Ejecute el mandato **backup** para copiar el archivo de configuración de IBM Tivoli Monitoring de la instancia de servidor SAP del directorio de agente sap1 a sap2. Especifique el nombre de archivo y sap1 como el sistema de origen desde el directorio del agente sap1. A continuación, se llama a la función ABAP que copia los valores de IBM Tivoli Monitoring de este archivo en el archivo de configuración de IBM Tivoli Monitoring para Sap2. A continuación, seleccione **`Copiar`** en la herramienta del programa de utilidad del directorio de agente sap1 y especifique un nombre de archivo y sap2 como el sistema SAP de destino.

- **Copia de seguridad**

  Después de ejecutar la herramienta de programa de utilidad de línea de mandatos, seleccione la opción **Copia de seguridad**. A continuación, es necesario especificar el nombre de archivo y el ID del sistema SAP. La herramienta llama al módulo de función SAP `/IBMMON/ITM_BACKUP`. El módulo de función lee los valores de configuración específicos de IBM Tivoli Monitoring almacenados en las tablas y los almacena con un separador de fila y columna. A continuación, la herramienta de programa de utilidad de línea de mandatos lee la serie y graba los datos en un archivo. El nombre de archivo que se genera tiene el siguiente formato: ID>_<nombre_archivo>-<fecha&hora>. Este archivo se almacena en el directorio en el que está almacenado el programa de utilidad.

- **Restaurar**

  Después de ejecutar la herramienta de programa de utilidad de línea de mandatos, especifique el nombre de archivo que va a restaurar y el sistema SAP de destino donde desea restaurar el archivo. La herramienta de programa de utilidad de línea de mandatos lee el archivo del directorio de agente y llama al módulo de función SAP `/IBMMON/ITM_RESTORE`. A continuación, la herramienta pasa las configuraciones de IBM Tivoli Monitoring como una serie. El módulo de función SAP actualiza las tablas específicas de IBM Tivoli Monitoring y restaura las configuraciones específicas de IBM Tivoli Monitoring.

Ejecución del programa de utilidad de línea de mandatos en un entorno Windows

Puede ejecutar el programa de utilidad de línea de mandatos en un entorno Windows para completar los procedimientos de copia, copia de seguridad y restauración.

Procedimiento

1. En función del sistema operativo, complete uno de los procedimientos siguientes:

- Para un sistema operativo de 64 bits, establezca la vía de acceso CANDLEHOME utilizando el mandato **set CANDLE_HOME = C:\IBM\APM** y ejecute el mandato **ksacopybackuprestore.bat** desde la siguiente vía de acceso: %candle_home%\TMAITM6x64.

2. Para crear un archivo de copia de seguridad, siga estos pasos:
   a) Seleccione **Copia de seguridad** y especifique el nombre de archivo y el nombre del sistema SAP de origen.
   b) El archivo de copia de seguridad se crea con el siguiente formato: SYS ID>_<nombre_archivo>_<fecha&hora>.
3. Para restaurar el archivo, siga estos pasos:
   a) Seleccione **Restaurar** y especifique el nombre del sistema SAP de destino.
   b) Especifique el nombre de archivo.
4. Para copiar el archivo, siga estos pasos:
   a) Desde el agente de origen, seleccione **Copia de seguridad** y cree un archivo de copia de seguridad.
   b) Copie el archivo de copia de seguridad del directorio del agente de origen en el directorio del agente de destino.
   c) Desde el directorio de origen, ejecute la herramienta de programa de utilidad de línea de mandatos y seleccione **Copiar**.
   d) Especifique el nombre de archivo y el sistema SAP de destino.

Ejecución del programa de utilidad de línea de mandatos en un entorno no Windows
Puede ejecutar el programa de utilidad de línea de mandatos en un entorno no de Windows para completar los procedimientos de copia, copia de seguridad y restauración.

Procedimiento

1. Ejecute el mandato **ksacopybackuprestore.sh** desde la vía de acceso siguiente: /candle_home/<arch>/sa/shell.
2. Para crear un archivo de copia de seguridad, siga estos pasos:
   a) Seleccione **Copia de seguridad** y especifique el nombre de archivo y el nombre del sistema SAP de origen.
   b) El archivo de copia de seguridad se crea con el siguiente formato: SYS ID>_<nombre_archivo>_<fecha&hora>.
      El archivo de copia de seguridad se guarda en esta ubicación: %candlehome% / arch /sa/bin.
3. Para restaurar el archivo, siga estos pasos:
   a) Seleccione **Restaurar** y especifique el nombre del sistema SAP de destino.
   b) Escriba el nombre de archivo.
4. Para copiar el archivo, siga estos pasos:
   a) Desde el agente de origen, seleccione **Copia de seguridad** y cree un archivo de copia de seguridad.
   b) Copie el archivo de copia de seguridad del directorio del agente de origen en el directorio del agente de destino.
   c) Desde el directorio de origen, ejecute la herramienta de programa de utilidad de línea de mandatos y seleccione **Copiar**.
   d) Especifique el nombre de archivo y el sistema SAP de destino.

Mantenimiento de alertas
Puede modificar las alertas que genera Tivoli Monitoring cambiando su estado y umbrales.

Esta transacción se utiliza para habilitar o inhabilitar las alertas generadas por Tivoli Monitoring y para establecer umbrales de aviso y críticos. Todas las alertas generadas por Tivoli Monitoring se muestran con sus valores de umbral y estado actuales.

Si modifica el estado y los umbrales de la alerta, los valores modificados se utilizarán en el siguiente periodo de muestra.

Mantenimiento del periodo de muestra predeterminado

El periodo de muestra predeterminado proporciona información sobre la creación de informes en tiempo real para determinados grupos de atributos.

Algunos grupos de atributos tienen una fecha y hora implícitas para cada registro del grupo. Por ejemplo, el grupo de atributos R/3_Abap_Dumps notifica la hora de creación del vuelco y el grupo de atributos R/3_System_Log notifica la hora de creación de la entrada de registro. Estos registros tienen un campo de fecha y hora. Puede obtener un informe de un breve historial de la tabla, en lugar de solo la información más reciente. Este intervalo es el periodo de tiempo de recopilación de datos y se utiliza como el intervalo de tiempo real durante la recopilación de datos. La transacción /IBMMON/ITM_PERIOD define un periodo de muestra predeterminado (intervalo de tiempo para la creación de informes en tiempo real) para cada uno de estos grupos de atributos. El periodo de muestra identifica la duración del periodo de muestra de datos que se inicia a partir de la hora actual y va hacia atrás.

Mantenimiento de los nombres de archivo de registro

En los informes de IBM Tivoli Monitoring con información de archivos de registro se incluyen archivos de registro específicos que coinciden sólo con instancias.

Esta transacción se utiliza para identificar qué archivos de registro se deben tener en cuenta para su inclusión en informes de IBM Tivoli Monitoring que contienen información de archivo de registro. Todos los archivos de registro cuyo nombre coincida con los patrones de nombre especificados en las instancias especificadas se incluirán en el informe en el siguiente intervalo de recopilación de datos.

Mantenimiento de grupo gestionado

La transacción de nombres de grupos gestionados supervisa y procesa transacciones específicas en el sistema SAP.

Utilice esta transacción para mantener definiciones de grupos gestionados de IBM Tivoli Monitoring. Todos los nombres de grupos gestionados se pasan al portal de la interfaz de usuario de IBM Application Performance Management y se muestran en las listas de selección de sistemas gestionados. En el momento de la recopilación de datos, solo se envían al agente de SAP los datos que coinciden con las condiciones de selección de atributos. Estos datos se muestran en los informes o se utilizan para la evaluación en situaciones y políticas.

Utilice los grupos gestionados para supervisar subconjuntos de información en el sistema SAP. Céntrese solo en las partes del sistema SAP que le interesen y omita aquellas partes que no le incumban. Por ejemplo, si solo está interesado en el tiempo de respuesta de las transacciones que forman parte de la aplicación financiera, cree un grupo gestionado denominado Datos financieros. A continuación, incluya en él únicamente códigos de transacciones financieras. Siempre que Tivoli Enterprise Portal procese el Grupo gestionado de entidades financieras, solo se tiene en cuenta la información que contiene los códigos de transacción especificados cuando se muestra un informe, se evalúa una situación o se evalúa una política.

Transacción Seleccionar conjuntos de supervisores y supervisores
Utilice la transacción Seleccionar conjuntos de supervisores y supervisores para editar la configuración de alertas de Centralized Computing Central Management (CCMS). Por ejemplo, puede desactivar completamente la recopilación de alertas de CCMS.

Esta transacción se utiliza para seleccionar los supervisores de CCMS de los que IBM Tivoli Monitoring recupera alertas. De forma predeterminada, el supervisor de sistema completo está seleccionado la primera vez que se muestra esta ventana. Puede cambiar el conjunto de supervisores, el supervisor, o el conjunto de supervisores y el supervisor, y a continuación guardar la configuración. Puede seleccionar un máximo de tres supervisores para los que recopilar alertas de CCMS.

Para desactivar completamente la recopilación de alertas de CCMS, desmarque el recuadro de selección para todos los supervisores y guarde esta configuración.

El agente que ya se está ejecutando lee esta configuración y recopila las alertas de CCMS para los supervisores seleccionados. De todos modos, las alertas de CCMS ya recopiladas por el agente antes de cambiar la configuración de alertas de CCMS se mantienen con el agente e IBM Tivoli Monitoring.

Además de seleccionar supervisores y conjuntos de supervisores, esta transacción especifica el número de apariciones de un tipo de alerta que se va a recuperar. Además, le ayuda a decidir si cerrar automáticamente las apariciones anteriores de alertas que no se han recuperado.

Configurar umbral de respuesta de paso del diálogo en el sistema SAP
Puede configurar un umbral de respuesta de paso de diálogo para cualquier transacción ejecutando la transacción SE16.

Procedimiento

1. En el campo **Nombre de tabla**, escriba `/IBMMON/ITM_TRSH` y, a continuación, seleccione **Contenido de tabla (F7)** para acceder a la tabla.
2. Para ver los valores del umbral actual, seleccione **Ejecutar (F8)**. Los nombres de transacción se muestran bajo la columna **WORKLOAD**; los valores de umbral se muestran bajo la columna **THRESHOLD**.
3. Para añadir un nuevo valor de umbral, seleccione **Crear (F5)**. Escriba el nombre de la transacción en el campo **WORKLOAD**. Para el valor **WORKLOAD**, se aceptan los comodines siguientes:
   - * coincide con varios caracteres
   - + coincide con cualquier carácter individual
4. Especifique el valor de umbral, en milisegundos, en el campo **THRESHOLD**. Seleccione **Guardar** para guardar este valor. Los valores de umbral nuevos y modificados no entran en vigor de inmediato, sino cuando se da alguna de estas condiciones:
   - Se reinicia el agente.
   - El agente reabre su conexión RFC al sistema SAP. Este procedimiento se produce cada 12 pulsaciones, lo que, de forma predeterminada, es aproximadamente cada 2 horas y 10 minutos.

Resultados
El valor especificado para la columna **Umbral** se devuelve en el atributo Umbral de respuesta de paso del diálogo del grupo de atributos R/3_Transaction_Performance.

Operaciones de trabajo por lotes
Puede captar todos los trabajos por lotes dentro de un intervalo de tiempo especificado.

Procedimiento

Siga los pasos indicados después de "Importación del transporte ABAP en el sistema SAP" en la página 763.

Recuerde: La Constante Crítica se establece para todos los trabajos por lotes.

1. Captar todos los trabajos por lotes activos y cancelados dentro de un intervalo de tiempo especificado.
   Añada la siguiente entrada en la tabla `/IBMMON/ITM_CNFG`.

Tabla 203. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
`BATCH_JOBS_PERF`	`SÍ`

2. Captar todos los trabajos cancelados dentro de un intervalo de tiempo especificado y todos los trabajos activos independientemente del intervalo de tiempo.
   Añada la siguiente entrada en la tabla `/IBMMON/ITM_CNFG`.

Tabla 204. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
BATCH_JOBS_PERF	YES_LONG_RUN

3. Captar todos los trabajos por lotes dentro de un intervalo de tiempo especificado y todos los trabajos por lotes activos independientemente del intervalo de tiempo.

   Añada la siguiente entrada en la tabla /IBMMON/ITM_CNFG.

Tabla 205. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
BATCH_JOBS_PERF	YES_ALL

Nota:

- Si no se añade el parámetro de configuración, capta todos los trabajos por lotes dentro de un intervalo de tiempo especificado sin la constante crítica establecida.
- El número de filas captadas es siempre igual al valor de la Constante Crítica establecida en el Código de transacción /n/IBMMON/ITM_CONFIG.

Mejora del rendimiento del módulo de función /IBMMON/ITM_MAIALRT_INX

Puede mejorar el rendimiento del módulo de función /IBMMON/ITM_MAIALRT_INX para Agente de SAP.

Procedimiento

Siga los pasos para mejorar el rendimiento del módulo de función /IBMMON/ITM_MAIALRT_INX.

1. Inicie la sesión en la interfaz gráfica de usuario de Agente de SAP.
2. Ejecute el código de transacción SE16 y escriba el nombre de tabla como /IBMMON/ITM_CNFG y pulse F7.
3. Pulse F5 o pulse **Crear entradas** y añada la siguiente entrada en la tabla IBMMON/ITM_CNFG.

Tabla 206. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
MAI_ALERTS_PERF	YES

Nota:

- Si la Constante Crítica no se ha establecido en el Código de transacción - /N/IBMMON/ITM_CONFIG, el valor predeterminado es 2500.
- Este proceso solo es aplicable para captar las alertas MAI del sistema SAP donde PERIOD_START y PERIOD_END es inicial.

  Recuerde: Ahora el módulo de función /IBMMON/ITM_MAIALRT_INX capta el número de alertas MAI equivalentes a la constante crítica establecida en el código de transacción - /N/IBMMON/ITM_CONFIG.
- Si esta entrada en el /IBMMON/ITM_CNFG no se crea de forma predeterminada, se captan las última 2500 alertas MAI.
- El número de filas captadas es siempre igual al valor de la Constante Crítica establecida en el Código de transacción /n/IBMMON/ITM_CONFIG.

Creación de informes del CCMS centralizado

Computing Center Management System (CCMS) centralizado es una prestación de supervisión de SAP.

Utilice esta prestación para notificar las alertas del CCMS de varios sistemas SAP a un concentrador de supervisión central. Puede supervisar el entorno SAP desde una única consola CCMS. La creación de informes del CCMS centralizado funciona mejor en estos entornos:

- Principalmente una operación de CCMS donde las alertas de CCMS son los únicos datos de supervisión necesarios.
- El CCMS centralizado forma parte del entorno SAP.
- Entornos SAP grandes con muchos sistemas SAP como por ejemplo ISV e ISP.
- Integración de IBM Tivoli Monitoring V5.x con adaptadores de CCMS de Agente de SAP.
- Recopilación de alertas de componentes y servidores de aplicaciones SAP que no sean ABAP.

El Agente de SAP da soporte a CCMS centralizado solo para la notificación de alertas. A continuación, puede colocar un Agente de SAP en un sistema SAP centralizado y ver las alertas CCMS para todo el entorno SAP. Este soporte se proporciona de varias formas:

- Al notificar las alertas de CCMS, el agente comprueba si las alertas están asociadas directamente al sistema SAP supervisado por el agente. Si el agente determina que una alerta pertenece a un sistema SAP distinto, presupone un CCMS centralizado y crea automáticamente sistemas gestionados R3_Group adicionales.
- El sistema gestionado <SID_local>-All_CCMS_alerts:Grp se utiliza para notificar el conjunto completo de alertas de todos los sistemas SAP remotos. El valor de <SID_local> es el identificador de sistema para el sistema SAP que se supervisa directamente. Por ejemplo, si el sistema SAP local es QA1, este nombre de grupo sería QA1-All_CCMS_alerts:Grp.
- El sistema gestionado <SID_local>-<SID_remoto>_CCMS_alerts:Grp se utiliza para notificar todas las alertas de un sistema SAP remoto. El valor de <SID_local> es el identificador de sistema para el sistema SAP que se supervisa directamente. El valor de <SID_remoto> es el identificador de sistema para el sistema SAP remoto. Por ejemplo, si el sistema SAP local es QA1 y el sistema SAP remoto es QA2, este nombre de grupo sería QA1-QA2_CCMS_alerts:Grp.
- Cada uno de estos sistemas gestionados en el árbol de Navigator tiene el conjunto completo de widgets en el mismo, pero solo los widgets de alertas tienen datos significativos.

El Agente de SAP mantiene sus definiciones de grupos del CCMS centralizado en el código de Advanced Business Application Programming (ABAP) del sistema SAP directamente gestionado. Es posible que deba modificar estas definiciones si un sistema SAP para el que está recibiendo alertas centralizadas también está siendo supervisado directamente por otra instancia del Agente de SAP. No desea que se notifiquen alertas en los dos sistemas. Puede limitar la notificación centralizada de alertas de la forma siguiente:

- Utilice la transacción `/IBMMON/ITM_CONFIG` para mantener grupos gestionados. Cambie el grupo Todas las alertas de CCMS. Elimine el sistema remoto de esta lista editando la definición del grupo para excluir el identificador del sistema remoto.
- Utilice la transacción `/IBMMON/ITM_CONFIG` para mantener grupos gestionados. Suprima el grupo de alertas de CCMS <SID_remoto>. Por ejemplo, si el sistema SAP remoto es QA2, el nombre de este grupo será Alertas de CCMS de QA2.

También puede utilizar el CCMS centralizado para notificar alertas de todos los sistemas SAP, pero impedir la notificación de alertas de cada uno de los agentes instalados localmente. Utilice los pasos siguientes para realizar esta configuración:

- Configure una instancia de Agente de SAP para supervisar el sistema CCMS centralizado. Permita que el agente detecte y notifique todas las alertas de todos los sistemas SAP remotos.
- Configure una instancia de Agente de SAP para supervisar cada sistema SAP remoto. Inhabilite la recopilación y notificación de alertas de estas instancias de agente utilizado la transacción /IBMMON/ITM_CONFIG para seleccionar conjuntos de supervisores y supervisores. En esta función, desmarque los recuadros de selección de todos los supervisores y guarde esta configuración.

El soporte de Agente de SAP para CCMS centralizado se utiliza en un entorno de supervisión puro del CCMS para ver todas las alertas de una consola común. También se puede utilizar con su conjunto completo de funciones para proporcionar situaciones, políticas y mandatos de actuación para los sistemas SAP remotos.

Desinstalación del transporte ABAP (Advanced Business Application Programming) del sistema SAP
Si opta por eliminar el Agente de SAP del sistema, debe importar el transporte Delete en el sistema SAP. El transporte Delete suprime los módulos de función y los objetos de diccionario del Agente de SAP.

Antes de empezar
Si el sistema SAP está en la versión 7.20 o posterior, antes de importar el transporte delete, en el perfil de transporte, tiene que añadir el siguiente parámetro del perfil de transporte: **tadirdeletions=true**. Este parámetro del perfil de transporte está disponible en la versión de tp 375.57.68 y en R3trans versión 6.14, release 700, o posterior. Para obtener más información sobre cómo eliminar las solicitudes de transporte del sistema SAP, consulte Supresión de solicitudes de transporte.

Procedimiento

1. Vaya al directorio /ABAP del CD del producto.
2. Copie los archivos de transporte en el entorno SAP.
3. Copie los archivos K711_00xxx_DELETE y R711_00xxx_DELETE en el directorio de datos del Sistema de transporte de SAP de la forma siguiente:
   a) Copie el archivo K711_00xxx_DELETE en el directorio cofiles.
   b) Copie el archivo R711_00xxx_DELETE en el directorio data.
4. Ejecute los mandatos siguientes:
   a) **tp addtobuffer ITMK711_00xxx_DELETE SID pf=\usr\sap\trans\bin ***NOMBRE_PERFIL*
   b) **tp import ITMK711_00xxx_DELETE SID client=nnn U16 pf=\usr\sap\trans\bin** *NOMBRE_PERFIL*

   Donde:

   SID
   ID del sistema SAP de destino

   NOMBRE_PERFIL
   Nombre del archivo de perfil de tp

   nnn
   Número del cliente de destino donde se ejecutará el agente

Personalización de instancias de SAP
De forma predeterminada, todas las instancias del sistema SAP se supervisan y se muestran en el portal de la interfaz de usuario de IBM Application Performance Management.

Como administrador, puede elegir qué instancia de SAP desea supervisar. Además, como administrador, puede desactivar una instancia de SAP que no desea supervisar.

La transacción personalizada /IBMMON/ITM_INSTANCE enlaza con la transacción /IBMMON/ITM_CONFIG.

Seleccione la opción **Instancias de SAP** para ver las instancias disponibles del servidor SAP. A continuación, seleccione la instancia que quiera supervisar. Estas instancias se visualizan en el portal de la interfaz de usuario de IBM Application Performance Management. Ninguna de las instancias inactivas o borradas se muestran en el portal de interfaz de usuario de IBM Application Performance Management.

Característica Probar conexión
La característica Probar conexión le permite comprobar que puede conectar el agente al sistema SAP que se está supervisando.

Puede especificar parámetros en la GUI para completar el procedimiento de conexión de prueba. Si se conecta correctamente al sistema SAP, se mostrará un mensaje de resultado satisfactorio. De forma alternativa, si esta conexión falla, se visualiza un mensaje de anomalía.

El botón **Probar conexión** solo está disponible en la ventana IBM Application Performance Management.

Habilitación del diseño de CCMS
La supervisión de Computing Center Management System (CCMS) se ha ampliado para recopilar registros CCMS que estén en estado abierto o cerrado desde el último periodo de muestra. Puede configurar el periodo de muestra; de forma predeterminada tiene un valor de 3 minutos. Sin embargo, debe asegurarse de que los archivos de transporte a los que hacen referencia el Agente de SAP y el transporte ABAP (Advanced Business Application Programming) sean de la misma versión.

Procedimiento

1. Inicie la sesión en el sistema SAP.
2. Abra la transacción SE16 y añada el nombre de tabla `/IBMMON/ITM_CNFG` a la transacción.
3. Para ejecutar el módulo de función ABAP `/IBMMON/ITM_CNFG` y proporcionar configuraciones para el programa ABAP, pulse **Intro** y a continuación pulse **F8**.
4. Para crear una nueva entrada a la que añadir nuevos parámetros de configuración, pulse **F5.**
5. Para crear un nuevo parámetro de configuración denominado **`ISNEWCCMSDESIGN`** con el valor *YES* en el servidor SAP, en el campo **PARM NAME** escriba `ISNEWCCMSDESIGN` y en el campo **VALUE CHAR**, escriba YES.
6. Pulse **Guardar**.

   Puede ignorar el campo VALUE INT.

Modificación del valor de umbral de una alerta
Puede modificar el valor de umbral **max ccms alert** asociado a una alerta. De forma predeterminada, el valor es 1000, lo que significa que puede ver 1000 alertas en IBM Application Performance Management. Las alertas más antiguas se eliminan de la memoria caché.

Procedimiento

1. Complete uno de los pasos siguientes:
   - En el sistema operativo Windows, abra el archivo `<inicio_candle>\tmaitm6\KSAENV`.
   - En un sistema operativo no Windows, abra el archivo `<inicio_candle>/config/sa.ini`.
2. Añada *MAX_CCMS_ALERT_THRESHOLD=<Valor>* al final del archivo.

   Nota: El valor debe ser mayor que 100.

Inhabilitación del diseño de CCMS
Puede inhabilitar el diseño de CCMS (Computing Center Management System).

Procedimiento

1. Inicie la sesión en el sistema SAP.
2. Abra la transacción SE16 y añada el nombre de tabla `/IBMMON/ITM_CNFG` a la transacción.
3. Para ejecutar el módulo de función ABAP `/IBMMON/ITM_CNFG` y proporcionar configuraciones para el programa ABAP, pulse **Intro** y a continuación pulse **F8**.
4. Para suprimir la entrada existente, seleccione y pulse con el botón derecho del ratón en **`ISNEWCCMSDESIGN`** y a continuación pulse **Suprimir**.

Configuración de la supervisión de base de datos SAP HANA

Debe configurar el Agente de SAP HANA Database para que el agente pueda recopilar datos del servidor de base de datos SAP HANA que se está supervisando.

Antes de empezar

Revise los requisitos previos de hardware y software, consulte Software Product Compatibility Reports para el agente de SAP HANA Database

A continuación se muestran los requisitos previos para configurar Agente de SAP HANA Database

1. Asegúrese de crear usuarios en todas las bases de datos (sistema y arrendatario) del sistema SAP HANA con los siguientes privilegios:
   - Rol: Supervisión
   - Privilegio de sistema: admin de supervisor

   El nombre de usuario y la contraseña para las bases de datos de sistema y arrendatario deben ser los mismos.
2. Cuando la conmutación entre la conectividad maestra a en espera tiene lugar en el sistema Agente de SAP HANA Database el agente utiliza el nombre de host del servidor en espera que es necesario resolver en el sistema de agente. Para resolver el nombre de host en una dirección IP, es necesario añadir una entrada de correlación en el archivo de host de la máquina en la que el agente está instalado.

Nota: Si configura el agente utilizando el host maestro, especifique el nombre de host completo o la dirección IP del host maestro. Si el usuario está configurando el agente utilizando Host en espera, especifique el nombre de host completo o la dirección IP del host en espera. Cuando configura el agente a través del nodo en espera, el nodo maestro debe estar inactivo junto con la máquina de host.

Acerca de esta tarea

El Agente de SAP HANA Database es un agente de múltiple instancia. Deberá crear la primera instancia e iniciar el agente manualmente.

Procedimiento

- Windows Para configurar el agente en sistemas Windows, realice los pasos siguientes:
  a) Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
  b) En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Plantilla** bajo la columna **Tarea/Subsistema** y pulse **Configurar utilizando los valores predeterminados**.

     Se abrirá la ventana **Monitoring Agent for SAP HANA Database**.
  c) En el campo **Especificar un nombre de instancia exclusivo**, escriba el nombre de una instancia del agente y pulse **Aceptar**.

     Importante: El nombre de instancia del agente debe coincidir con el identificador de sistema de base de datos HANA de 3 dígitos (SID). Por ejemplo, si el SID de la base de datos SAP HANA gestionada es H01, especifique H01 como nombre de instancia.
  d) En la ventana **Monitoring Agent for SAP HANA Database**, especifique valores para los campos siguientes:

     Nombre de instancia
     El valor predeterminado para este campo es igual que el valor que se especifica en el campo **Especificar un nombre de instancia exclusivo**.

     Nombre de servidor
     El nombre de host completo o la dirección IP del servidor SAP HANA en el que está instalada la base de datos del sistema.

     Nombre de base de datos
     El nombre de la base de datos SAP HANA.

     Número de puerto
     El número de puerto SQL del servicio de servidor de índices de la base de datos del sistema del servidor de bases de datos SAP HANA.

     Administrador de la base de datos HANA
     El nombre de usuario para acceder al servidor de bases de datos SAP HANA.

     Contraseña del administrador de la base de datos HANA
     La contraseña para acceder al servidor de bases de datos SAP HANA.

Confirmar contraseña del administrador de la base de datos HANA
La contraseña que se especifica en el campo **Contraseña del administrador de la base de datos HANA**.

e) Pulse **Aceptar**.

f) En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón la instancia de agente que ha creado y pulse **Iniciar**.

- Linux AIX Para configurar el agente en sistemas Linux o AIX, realice los pasos siguientes:

  a) En la línea de mandatos, cambie la vía de acceso al directorio de instalación de agente.
  Ejemplo: `/opt/ibm/apm/agent/bin`

  b) Ejecute el mandato siguiente, donde nombre_instancia es el nombre que asignará a la instancia:
  `./sap_hana_database-agent.sh config` *`nombre_instancia`*

  Importante: El nombre de instancia debe coincidir con el identificador de sistema de base de datos HANA de 3 dígitos (SID). Si el SID de la base de datos SAP HANA gestionada es H01, especifique `H01` como nombre de instancia.

  c) Cuando la línea de mandatos muestre el siguiente mensaje, escriba 1 y pulse Intro: `Edit 'Monitoring Agent for SAP HANA Database' setting? [1=Yes, 2=No]`

  d) Especifique valores para los parámetros de agente siguientes:

  Nombre de servidor
  El nombre de host completo o la dirección IP del servidor SAP HANA en el que está instalada la base de datos del sistema.

  Nombre de base de datos
  El nombre de la base de datos SAP HANA.

  Número de puerto
  El número de puerto SQL del servicio de servidor de índices de la base de datos del sistema del servidor de bases de datos SAP HANA.

  Administrador de la base de datos HANA
  El nombre de usuario para acceder al servidor de bases de datos SAP HANA.

  Contraseña del administrador de la base de datos HANA
  La contraseña para acceder al servidor de bases de datos SAP HANA.

  Confirmar contraseña del administrador de la base de datos HANA
  La contraseña que se especifica en el campo **Contraseña del administrador de la base de datos HANA**.

  e) Ejecute el mandato siguiente para iniciar el Agente de SAP HANA Database:
  `./sap_hana_database-agent.sh start` *`nombre_instancia`*

- Para configurar el agente utilizando el archivo de respuestas silencioso, siga estos pasos:

  a) En un editor de texto, abra el archivo `sap_hana_silent_config.txt` que está disponible en la vía de acceso *`dir_instalación`*`\samples` y especifique valores para todos los parámetros.

  Windows `C:\IBM\APM\samples`

  Linux AIX `/opt/ibm/apm/agent/samples`

  b) En la línea de mandatos, cambie la vía de acceso a *`dir_instalación`*`\bin`

  c) Ejecute el mandato siguiente:

  Windows `sap_hana_database-agent.bat config` *`nombre_instancia`* *`dir_instalación`*`\samples\sap_hana_silent_config.txt`

  Linux AIX `sap_hana_database-agent.sh config` *`nombre_instancia`* *`dir_instalación`*`\samples\sap_hana_silent_config.txt`

  d) Inicie el agente.

Windows En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón la instancia de agente que ha creado y pulse **Iniciar**.

Linux AIX Ejecute el mandato siguiente: `./sap_hana_database-agent.sh start nombre_instancia`

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración de la supervisión de SAP NetWeaver Java Stack

Debe configurar el Agente de SAP NetWeaver Java Stack para que el agente pueda recopilar datos de supervisor de recursos del servidor de aplicaciones SAP NetWeaver que se está supervisando. Para supervisar datos de diagnósticos y rastreo de transacciones, debe realizar algunas tareas de configuración.

Antes de empezar

Revise los requisitos previos de hardware y software, consulte Software Product Compatibility Reports para el agente SAP NetWeaver Java Stack

Asegúrese de realizar las siguientes tareas de requisito previo antes de configurar el agente:

- Copie los siguientes archivos JAR en el directorio `bin`:
  - `sapj2eeclient.jar` (la API de cliente del motor SAP J2EE que incluye el adaptador JMX)
  - `logging.jar` (la biblioteca de registro)
  - `com_sap_pj_jmx.jar` (la biblioteca SAP-JMX)
  - `exception.jar` (la infraestructura de excepción SAP)

  El directorio `bin` se encuentra en la vía de acceso siguiente:

  Windows `candle_home\TMAITM6_x64`

  Linux `candle_home/interp/sv/bin`

  Importante: Los archivos JAR son los mismos para todos los sistemas operativos soportados. Estos archivos están disponibles en el parche del agente de diagnóstico o el gestor de actualizaciones de software (SUM).
- En Variables de entorno, añada *<candleHome>\svdchome\<número de compilación>\toolkit\lib\win64\ttapi* a la variable de vía de acceso.
- Asigne el rol NWA_READONLY al usuario *Guest* (invitado) para recopilar los datos de diagnósticos y rastreo de transacciones.

Acerca de esta tarea

El Agente de SAP NetWeaver Java Stack es un agente de múltiple instancia. Deberá crear la primera instancia e iniciar el agente manualmente.

- Para configurar el agente en sistemas Windows, puede utilizar la GUI o el archivo de respuestas silencioso.

- Para configurar el agente en sistemas Linux o AIX, puede utilizar la línea de mandatos o el archivo de respuestas silencioso.

Para configurar la recopilación de datos de diagnóstico y rastreo de transacciones, realice las tareas siguientes:

1. Configure el recopilador de datos. Para obtener detalles, consulte "Configuración del recopilador de datos" en la página 795.
2. Habilite la recopilación de datos de diagnóstico y rastreo de transacciones. Para obtener detalles, consulte "Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones" en la página 797.

Las instrucciones indicadas en este tema son para el release más reciente del agente, excepto que se indique lo contrario. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Versión de agente.

Configuración del agente en sistemas Windows

Puede configurar el agente en sistemas operativos Windows mediante la ventana **IBM Performance Management**.

Antes de empezar

Asegúrese de que los archivos que están listados en la sección "Antes de empezar" del tema "Configuración de la supervisión de SAP NetWeaver Java Stack" en la página 792 están disponibles en el directorio `bin`.

Acerca de esta tarea

El Agente de SAP NetWeaver Java Stack proporciona valores predeterminados para algunos parámetros. Puede especificar diferentes valores para estos parámetros.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Plantilla** en la columna **Tarea/Subsistema** y pulse **Configurar agente**.

   Se abre la ventana **Monitoring Agent for SAP NetWeaver Java Stack**.
3. En el campo **Especificar un nombre de instancia exclusivo**, escriba el nombre de una instancia del agente y pulse **Aceptar**.

   Importante: El nombre de instancia del agente debe coincidir con el identificador de sistema de pila (SID) Java SAP NetWeaver de 3 dígitos. Por ejemplo, si el SID de la pila Java SAP NetWeaver gestionada es P14, especifique P14 como nombre de instancia.
4. En la ventana **Monitoring Agent for SAP NetWeaver Java Stack**, especifique valores para los parámetros de configuración y pulse **Aceptar**.

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 799.
5. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón la instancia de agente que ha creado y pulse **Iniciar**.

Qué hacer a continuación

- Inicie sesión en la Consola de Cloud APM para ver los datos de supervisión de recursos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte Inicio de la consola de Performance Management.
- Para recopilar datos de diagnósticos y rastreo de transacciones, configure el recopilador de datos y habilite la recopilación de datos para los diagnósticos y el rastreo de transacciones.

Configuración del agente en sistemas Linux o AIX

Para configurar el agente en sistemas Linux o AIX, debe ejecutar el script y responder a las solicitudes.

Antes de empezar

Asegúrese de que los archivos que están listados en la sección "Antes de empezar" del tema “Configuración de la supervisión de SAP NetWeaver Java Stack” en la página 792 están disponibles en el directorio `bin`.

Procedimiento

1. En la línea de mandatos, cambie la vía de acceso al directorio de instalación de agente.

   Linux `/opt/ibm/apm/agent/bin`

   Linux AIX `/opt/ibm/apm/agent/bin`
2. Ejecute el mandato siguiente:

   `./sap_netweaver_java_stack-agent.sh config` *`nombre_instancia`*

   donde *nombre_instancia* es el nombre que desea proporcionar a la instancia.

   Importante: El nombre de instancia del agente debe coincidir con el identificador de sistema de pila (SID) Java SAP NetWeaver de 3 dígitos. Por ejemplo, si el SID de la pila Java SAP NetWeaver gestionada es P14, especifique P14 como nombre de instancia.
3. Cuando la línea de mandatos muestra el siguiente mensaje, escriba 1 y pulse Intro.

   `¿Desea editar el valor ‘Monitoring Agent for la pila Java de SAP NetWeaver’? [1=Yes, 2=No]`
4. Cuando se le solicite, especifique valores para los parámetros de configuración.

   Para obtener más información sobre los parámetros de configuración, consulte “Parámetros de configuración del agente” en la página 799
5. Ejecute el mandato siguiente para iniciar el agente:

   `./sap_netweaver_java_stack-agent.sh start` *`nombre_instancia`*

Qué hacer a continuación

- Inicie sesión en la Consola de Cloud APM para ver los datos de supervisión de recursos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte Inicio de la consola de Performance Management.
- Para recopilar datos de diagnósticos y rastreo de transacciones, configure el recopilador de datos y habilite la recopilación de datos para los diagnósticos y el rastreo de transacciones.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Antes de empezar

Asegúrese de que los archivos que están listados en la sección "Antes de empezar" del tema “Configuración de la supervisión de SAP NetWeaver Java Stack” en la página 792 están disponibles en el directorio `bin`.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

1. En un editor de texto, abra el archivo `sap_netweaver_java_stack_silent_config.txt` que está disponible en la vía de acceso siguiente y especifique valores para todos los parámetros de configuración.

   Windows `C:\IBM\APM\samples`

   Linux AIX `/opt/ibm/apm/agent/samples`

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 799
2. En la línea de mandatos, cambie la vía de acceso a `dir_instalación\bin`
3. Ejecute el mandato siguiente:

   Windows `sap_netweaver_java_stack-agent.bat config` *`nombre_instancia`* `dir_instalación\samples\sap_netweaver_java_stack_silent_config.txt`

   Linux AIX `./sap_netweaver_java_stack-agent.sh config` *`nombre_instancia`* `dir_instalación\samples\sap_netweaver_java_stack_silent_config.txt`
4. Inicie el agente.

   Windows En la ventana de IBM Cloud Application Performance Management, pulse con el botón derecho del ratón la instancia de agente que ha creado y pulse **Iniciar**. Como alternativa, también puede ejecutar el mandato siguiente: `sap_netweaver_java_stack-agent.bat start` *`nombre_instancia`*

   Linux AIX Ejecute el mandato siguiente `./sap_netweaver_java_stack-agent.sh start` *`nombre_instancia`*

Qué hacer a continuación

- Inicie sesión en la Consola de Cloud APM para ver los datos de supervisión de recursos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte Inicio de la consola de Performance Management.
- Para recopilar datos de diagnósticos y rastreo de transacciones, configure el recopilador de datos y habilite la recopilación de datos para los diagnósticos y el rastreo de transacciones.

Configuración del recopilador de datos

Puede configurar el recopilador de datos para cada instancia de servidor de aplicaciones que desee supervisar.

Antes de empezar

Asegúrese de que los archivos que están listados en la sección "Antes de empezar" del tema "Configuración de la supervisión de SAP NetWeaver Java Stack" en la página 792 están disponibles en el directorio `bin`.

Procedimiento

Para configurar el recopilador de datos respondiendo a solicitudes, siga estos pasos:

1. En la línea de mandatos, cambie la vía de acceso por el directorio Windows `dir_instalación\svdchome\build no\bin\configNW` o Linux AIX `dir_instalación/svdchome/build no/bin/configNW` y ejecute el script siguiente:

   Windows config.bat

   Linux AIX config.sh
2. Seleccione la versión de NetWeaver Server especificando el número correspondiente al producto para el que desea configurar el recopilador de datos y pulse Intro.
3. Cuando se le solicite un nombre de usuario, especifique el nombre de usuario configurado en SAP NetWeaver Application Server with Java Stack y pulse Intro.
4. Cuando se le solicite la contraseña, especifique la contraseña y pulse Intro.
5. Cuando se le solicite que vuelva a especificar la contraseña, especifíquela de nuevo y pulse Intro.
6. Cuando se le solicite un número de puerto P4, especifique el número de puerto P4 de la instancia de SAP NetWeaver Application Server disponible en el sistema local y pulse Intro.

   Importante: utilice esta fórmula para calcular el número de puerto P4: 50000 + (número instancia*100) + 4
7. Cuando se le solicite que seleccione el número de instancia de NetWeaver Server, especifique número correspondiente a la instancia que desea configurar y pulse Intro.

   Recuerde: debe configurar el recopilador de datos por separado para cada instancia.
8. Si se le solicita que especifique la vía de acceso al directorio de inicio de Java, utilice JAVA_HOME de la instancia de SAP. Por ejemplo, `E:\usr\sap\J01\J04\exe\sapjvm_6`.
9. Cuando se le solicite, especifique 1 si desea habilitar la recopilación de datos de rastreo de transacciones. De lo contrario, especifique 2 y pulse Intro.
10. Cuando se le solicite, especifique 1 si desea habilitar la recopilación de datos de diagnóstico. De lo contrario, especifique 2 y pulse Intro.

Resultados

Se generará la vía de acceso para cargar los archivos de clase.

Qué hacer a continuación

1. Añada la vía de acceso generada a la variable de entorno adecuada.

   Windows *PATH*

   Linux *LD_LIBRARY_PATH* y *LIBPATH*

   AIX *LD LIBRARY PATH* y *LIB PATH*

   Recuerde:

   Windows Añada la vía de acceso generada a la variable de entorno *PATH*.

   Linux Añada la vía de acceso generada a *LD_LIBRARY_PATH* y *LIBPATH* en el archivo `/home/sidadm/.cshrc` del formato siguiente.

   ```
   setenv LD_LIBRARY_PATH /path
   setenv LIBPATH /path
   ```

   AIX Añada la vía de acceso generada a *LD LIBRARY PATH* y *LIB PATH* en el archivo `/etc/environment` en el formato siguiente.

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/path
   LIBPATH=$LIBPATH:/path
   ```
2. Reinicie las instancias del servidor de aplicaciones.

3. Habilite la recopilación de datos para el rastreo de transacciones y diagnóstico. Para obtener detalles, consulte "Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones" en la página 797.

Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones

En la página **Configuración de agente**, puede habilitar o inhabilitar la recopilación de datos para el rastreo de transacciones o diagnóstico.

Antes de empezar

Asegúrese de que el recopilador de datos esté configurado. Para obtener detalles, consulte "Configuración del recopilador de datos" en la página 795.

Acerca de esta tarea

Si habilita la recopilación de datos de rastreo de transacciones, el agente recopila datos de los componentes siguientes:

- Servlet JSP
- RemoteEJB
- JMS

Procedimiento

Complete los pasos siguientes para configurar la recopilación de datos para cada instancia de SAP NetWeaver Application Server.

1. Inicie la sesión en la Consola de Cloud APM.
2. En la barra de navegación, pulse **Configuración del sistema** > **Configuración del agente**.
   Se mostrará la página **Configuración del agente**.
3. Pulse la pestaña **NetWeaver**.
4. Marque los recuadros de selección de las instancias de SAP NetWeaver Application Server para las que desea configurar la recopilación de datos y lleve a cabo una de las acciones siguientes de la lista **Acciones**.
   - Para habilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Habilitado**. El estado de la columna **Rastreo de transacciones** se actualiza a Habilitado para cada instancia de SAP NetWeaver Application Server seleccionada.
   - Para habilitar la recopilación de datos de diagnóstico, seleccione **Establecer modalidad de diagnóstico** > **Sólo Modalidad de diagnóstico habilitada**. El estado de la columna Modalidad de diagnóstico se actualiza a Habilitado para cada instancia de SAP NetWeaver Application Server seleccionada.
   - Para habilitar la recopilación de datos de diagnóstico y el rastreo de método, seleccione **Establecer modalidad de diagnóstico** > **Modalidad de diagnóstico y rastreo de método habilitados**. El estado de las columnas Modalidad de diagnóstico y Rastreo de método se actualiza a Habilitado para cada instancia de SAP NetWeaver Application Server seleccionada.
   - Para inhabilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Inhabilitado**. El estado de la columna **Rastreo de transacciones** se actualiza a Inhabilitado para cada instancia de SAP NetWeaver Application Server seleccionada.
   - Para inhabilitar la recopilación de datos de diagnóstico, pulse **Establecer la modalidad de diagnóstico** > **Modalidad de diagnóstico y rastreo de método inhabilitados**. El estado de las columnas **Modalidad de diagnóstico y Rastreo de método** se actualiza a Inhabilitado para cada instancia de SAP NetWeaver Application Server seleccionada.

Resultados

La recopilación de datos se ha configurado para cada instancia de SAP NetWeaver Application Server.

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos de diagnóstico y rastreo de transacciones recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte “Inicio de la Consola de Cloud APM” en la página 1009.

Eliminación de la configuración del recopilador de datos

Puede retrotraer los cambios realizados al configurar el recopilador de datos para una instancia de SAP Netweaver Application Server with Java Stack.

Procedimiento

Para eliminar la configuración del recopilador de datos respondiendo a solicitudes, siga estos pasos:

1. En la línea de mandatos, cambie la vía de acceso por el directorio Windows `dir_instalación\svdchome\build no\bin\configNW` o Linux AIX `dir_instalación/svdchome/build no/bin/configNW` y ejecute el script siguiente:

   Windows unconfig.bat

   Linux AIX unconfig.sh

   Se listarán todas las instancias para las que el recopilador de datos está configurado.
2. Especifique el número correspondiente a la instancia de la que desea eliminar la configuración del recopilador de datos y pulse Intro.

   Consejo: para eliminar la configuración de recopilador de datos de varias instancias, especifique los números correspondientes a las instancias separados por comas. Para eliminar la configuración del recopilador de datos de todas las instancias, puede ejecutar los scripts siguientes:

   Windows config.bat -a

   Linux AIX config.sh -a

Qué hacer a continuación
Reinicie las instancias de SAP NetWeaver AS with Java Stack.

Restauración de la instancia de SAP NetWeaver Application Server

Puede utilizar el programa de utilidad de restauración para restaurar los parámetros de JVM si la instancia de SAP NetWeaver Application Server no se inicia después de la configuración de SAP NetWeaver Data Collector o para restaurar la instancia de SAP NetWeaver Application Server.

Procedimiento

Para restaurar la instancia de SAP NetWeaver Application Server respondiendo a solicitudes, siga estos pasos:

1. En la línea de mandatos, cambie la vía de acceso por el directorio Windows `dir_instalación\svdchome\build no\bin\configNW` o Linux AIX `dir_instalación/svdchome/build no/bin/configNW` y ejecute el script siguiente:

   Windows `restoreNW.bat`

   Linux AIX `restoreNW.sh`
2. Seleccione la versión de NetWeaver Server especificando el número que corresponde al producto para el que desea restaurar los parámetros de JVM y pulse Intro.
3. Cuando se le solicite un nombre de usuario, especifique el nombre de usuario para la instancia de SAP NetWeaver Application Server y pulse Intro.
4. Cuando se le solicite la contraseña de usuario, especifique la contraseña de usuario para la instancia de SAP NetWeaver Application Server y pulse Intro.

5. Cuando se le solicite un número de puerto P4, especifique el número de puerto P4 de la instancia de SAP NetWeaver Application Server disponible en el sistema local y pulse Intro.

   Si la información de instancia no se encuentra utilizando el puerto P4 especificado, se visualizará el mensaje `No ha podido establecerse conexión con SAP NetWeaver Server` y se le pedirá que proporcione la vía de acceso al directorio inicial de la instancia de NetWeaver Server.

   Por ejemplo, `usr\sap\`*`Nombre_Sistema`*`\`*`Número_Instancia`*
6. Cuando se le solicite que seleccione el número de instancia de NetWeaver Server, especifique el número que corresponde a la instancia que desea restaurar y pulse Intro.

Resultados

Se visualizará el mensaje siguiente:

```
Restauración satisfactoria. Reinicie la instancia.
```

Parámetros de configuración del agente

Al configurar el Agente de SAP NetWeaver Java Stack, puede cambiar el valor predeterminado de los parámetros, como por ejemplo SAP_NETWEAVER_P4_HOSTNAME y SAP_NETWEAVER_P4_PORT.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del Agente de SAP NetWeaver Java Stack. Debe especificar un valor para todos los campos, ya que son obligatorios.

Tabla 207. Nombres y descripciones de los parámetros de configuración

Nombre de parámetro	Descripción
Nombre de instancia	El nombre de la instancia. El valor predeterminado para este campo es igual que el valor que se especifica en el campo **Especificar un nombre de instancia exclusivo**.
SAP_NETWEAVER_P4_ HOSTNAME	Nombre de host o dirección IP del servidor de aplicaciones SAP NetWeaver.
SAP_NETWEAVER_P4_ PORT	El número de puerto P4 del SAP NetWeaver Application Server.
SAP_NETWEAVER_P4_ USERNAME	Nombre de usuario del administrador para acceder al servidor de aplicaciones SAP NetWeaver.
SAP_NETWEAVER_P4_ PASSWORD	Contraseña del administrador para acceder al servidor de aplicaciones SAP NetWeaver.
Confirmar SAP_NETWEAVER_P4_ PASSWORD	Contraseña especificada para el parámetro **SAP_NETWEAVER_P4_PASSWORD**.

Configuración de la supervisión de Siebel

El Agente de Siebel proporciona un punto central de supervisión de los recursos de Siebel, que incluyen estadísticas de Siebel, sesiones de usuario, componentes, tareas, servidor de la aplicaciones, Servidor de nombres de pasarela de Siebel, uso de memoria y CPU de proceso y supervisión de sucesos de registro.

Antes de empezar

- Lea todo el tema "Configuración de la supervisión de Siebel" en la página 799 para determinar qué se necesita para completar la configuración.
- Las instrucciones siguientes son para el release más reciente del agente, a excepción de lo indicado.

- Asegúrese de que los requisitos del sistema del Agente de Siebel se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Siebel.
- Antes de configurar el Agente de Siebel, debe verificar la cuenta de usuario de Siebel utilizada por el Agente de Siebel.

La habilitación de la supervisión por estadísticas de componente está inhabilitada de forma predeterminada. Puede habilitar la supervisión por estadísticas de componente.

Acerca de esta tarea

El Agente de Siebel es un agente de varias instancias. Deberá crear la primera instancia e iniciar el agente manualmente.

Procedimiento

1. Para configurar el agente en sistemas Windows, puede utilizar la ventana IBM Performance Management o el archivo de respuestas silencioso.
   - "Configuración del agente en sistemas Windows" en la página 802.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 807.
2. Para configurar el agente en sistemas Linux y UNIX, puede ejecutar el script y responder a solicitudes o utilizar el archivo de respuestas silencioso.
   - "Configuración del agente respondiendo a solicitudes" en la página 806.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 807.

Qué hacer a continuación

En Consola de Cloud APM, vaya a las páginas de Panel de instrumentos del rendimiento de aplicaciones para ver los datos recopilados. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si no puede ver los datos en los paneles de instrumentos del agente, consulte primero los registros de conexión del servidor y, a continuación, los registros del proveedor de datos. Las vías de acceso predeterminadas a estos registros son los siguientes:

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Si desea recibir ayuda con la resolución de problemas, consulte el Foro de Cloud Application Performance Management.

Verificar la cuenta de usuario de Siebel

Debe verificar la cuenta de usuario utilizada para ejecutar el agente de Siebel antes de configurar el agente.

Acerca de esta tarea

La cuenta de usuario utilizada para ejecutar el Agente de Siebel debe tener permisos para ejecutar el programa de utilidad de línea de mandatos **srvrmgr** de Siebel. Para verificar que la cuenta de usuario tiene los permisos necesarios, siga estos pasos:

Procedimiento

1. Inicie la sesión en el sistema con la cuenta de usuario utilizada para ejecutar el Agente de Siebel.
2. Cambie de directorio a la ubicación donde está instalado el servidor Siebel.
3. Ejecute source sobre el archivo de entorno de Siebel:

   ```
   source siebenv.sh
   ```

4. Ejecute el mandato siguiente:

```
srvrmgr /s servidor_Siebel /g pasarela_Siebel /e empresa_Siebel
/u cuenta_usuario /p contraseña
/c "list servers"
```

donde

servidor_Siebel
Nombre del servidor de aplicaciones Siebel.

pasarela_Siebel
Nombre del servidor de nombres de pasarela activo actualmente.

empresa_Siebel
Nombre de la empresa de Siebel.

cuenta_usuario
Cuenta de usuario que se utiliza para iniciar la sesión en el sistema.

contraseña
Contraseña que está asociada con la cuenta de usuario.

Si la cuenta de usuario tiene los permisos necesarios, verá una salida similar al ejemplo siguiente, en la que los campos devueltos están limitados a tres:

```
Connected to 1 server(s) out of a total of 1 server(s) in the enterprise

srvrmgr:s82win8> list servers show SBLSRVR_NAME, HOST_NAME, SBLSRVR_STATUS

SBLSRVR_NAME  HOST_NAME  SBLSRVR_STATUS
------------  ---------  --------------------------------
s82win8       s82win8    16.0.0.0 [23057] LANG_INDEPENDENT

1 row returned.
```

Si el mandato **srvrmgr** no se ejecuta correctamente, consulte al administrador de Siebel del servidor. Asegúrese de haber definido las variables del entorno de Siebel requeridas para la cuenta de usuario, así como que la cuenta de usuario cuenta con los permisos correctos para ejecutar el mandato **srvrmgr**.

Habilitación de la supervisión por estadísticas de componente

La habilitación de la supervisión por estadísticas de componente está inhabilitada de forma predeterminada. Puede habilitar la supervisión por estadísticas de componente utilizando la variable de entorno KUY_ENABLE_COMP_STATS.

Antes de empezar

Debido a un problema conocido con servidores de Siebel V8.1 y versiones posteriores, la recopilación de estadísticas de componente de Siebel puede tener un efecto negativo sobre el uso de la memoria del servidor de pasarela de Siebel. Este problema se aborda en la nota técnica publicada por Oracle denominada "Gateway Service on Siebel 8.1 or 8.2 Might Consume High Memory Consumption: Recovery (Doc ID 1269177.1)". En dicho artículo se proporciona un arreglo para el problema. El arreglo se implementa en el servidor Siebel.

Si la supervisión de estadísticas por componente es necesaria en el entorno, aplique el arreglo de Oracle a los Servidores de pasarela de Siebel V8.1 y posteriores antes de habilitar la supervisión de estadísticas por componente.

Acerca de esta tarea

Tras aplicar el arreglo de Oracle, siga estos pasos para habilitar la supervisión de estadísticas por componente en el Agente de Siebel:

Procedimiento

1. Vaya al directorio de instalación de agente del Agente de Siebel:
   - Windows *dir_instalación*\TMAITM6_x64
   - Linux AIX *dir_instalación*/config
2. Edite el archivo de configuración del Agente de Siebel para establecer KUY_ENABLE_COMP_STATS en true.
   - Windows KUYENV_*nombre_instancia*
   - Linux AIX uy.environment

   donde *nombre_instancia* es el nombre de instancia del agente de Siebel.
3. Reinicie el agente.

   Importante: Para que este sea el valor predeterminado para todas las instancias de agente nuevas, establezca KUY_ENABLE_COMP_STATS en true en los archivos de plantilla de configuración:
   - Windows KUYENV
   - Linux AIX Este valor ya se convierte en el valor predeterminado de las instancias de agente nuevas editando uy.environment en el Paso 2.

Configuración del agente en sistemas Windows

Puede configurar el Agente de Siebel en sistemas operativos Windows utilizando la ventana de IBM Cloud Application Performance Management. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la plantilla **Monitoring Agent for Siebel** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar una instancia de agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar la instancia de agente de nuevo, púlsela con el botón derecho del ratón y luego pulse **Reconfigurar**.
3. Especifique un nombre de instancia exclusivo y luego pulse **Aceptar**. Utilice solamente letras, números, el carácter de subrayado y el carácter menos en el nombre de la instancia. Por ejemplo: siebel01.

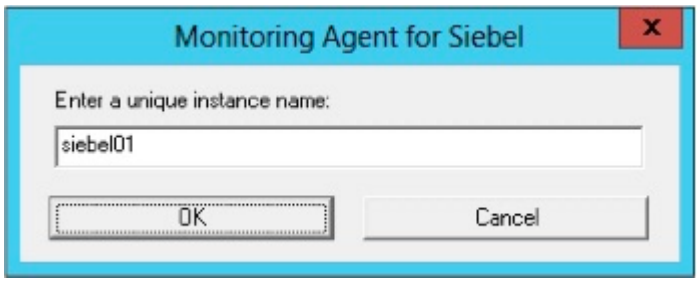


Figura 22. La ventana para especificar un nombre de instancia exclusivo.

4. Seleccione un tipo de servidor, especifique valores para los campos necesarios para dicho tipo de servidor y, a continuación, pulse **Siguiente**.

   Consulte la sección Tabla 208 en la página 808 para obtener una descripción de cada uno de los parámetros de configuración.

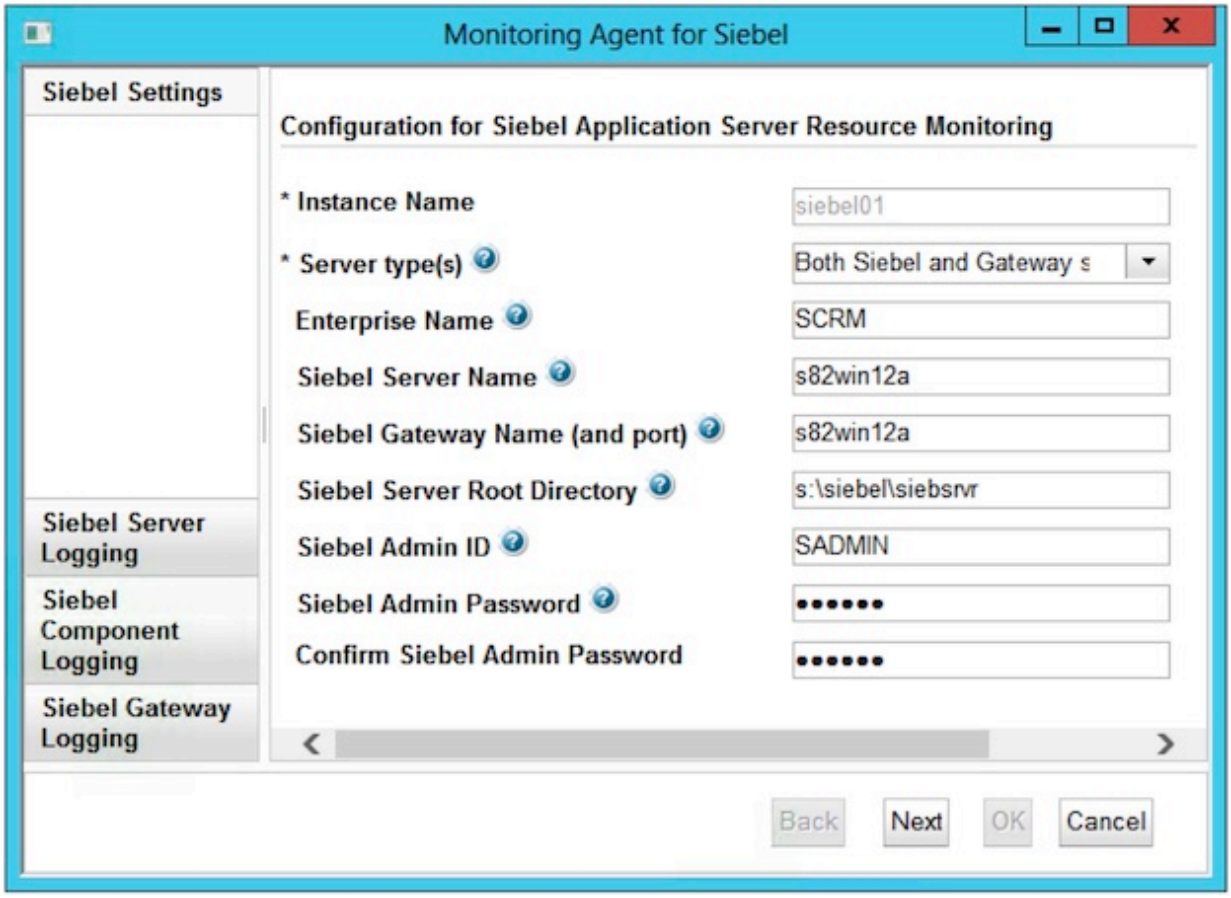


Figura 23. La ventana de los parámetros de configuración para los tipos de servidores Siebel instalados en un host Siebel

Importante: si el Agente de Siebel está instalado en un sistema con el Servidor de nombres de pasarela de Siebel pero sin el servidor Siebel, los datos que se visualizan en el Panel de instrumentos de aplicaciones sólo son aplicables al Servidor de nombres de pasarela de Siebel para esta instancia. Todas las demás vistas de Agente de Siebel están vacías.

5. Opcional: Edite los valores para el registro del servidor Siebel y pulse **Siguiente**.

   Consulte la sección Tabla 209 en la página 809 para obtener una descripción de cada uno de los parámetros de configuración.

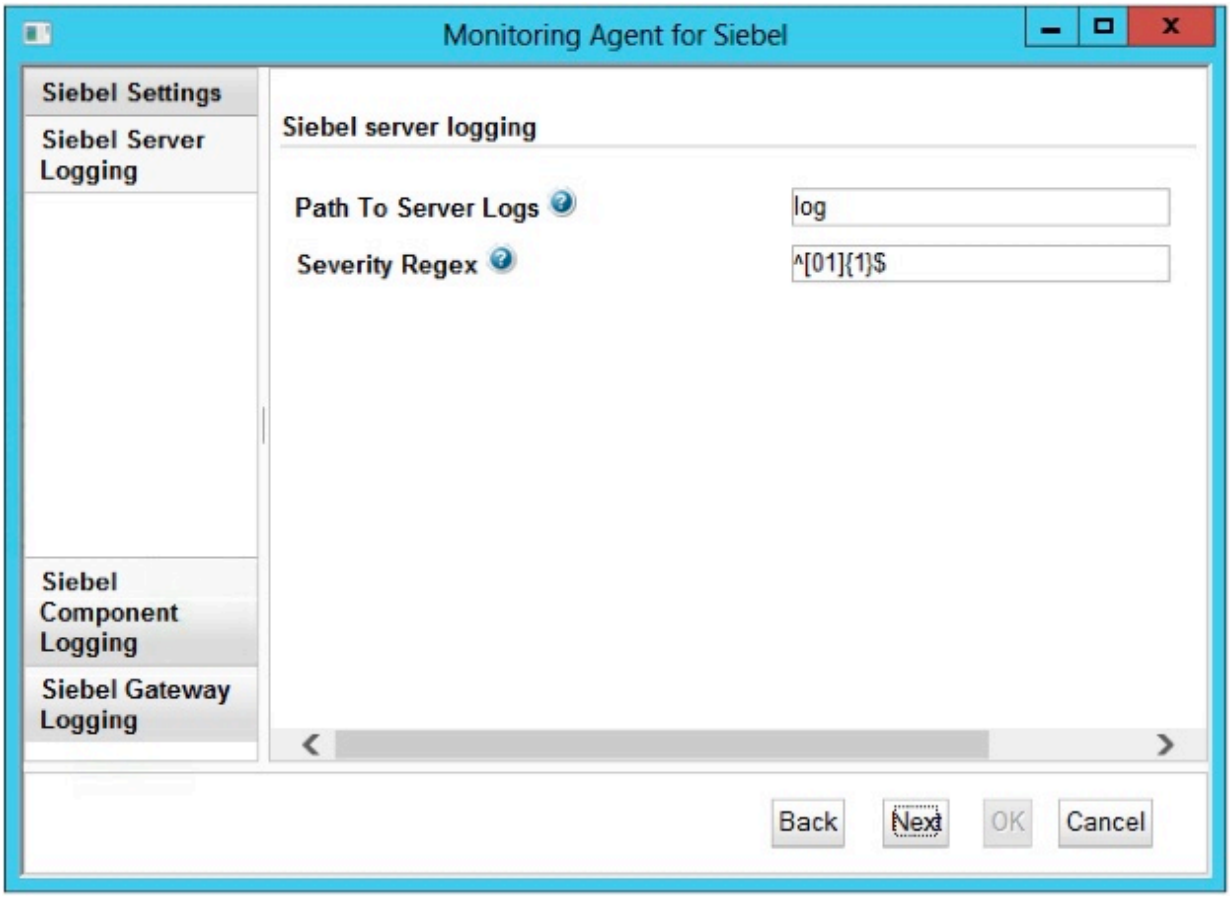


Figura 24. La ventana para especificar valores de registro del servidor Siebel.

6. Opcional: Edite los valores para el registro de componentes de Siebel y pulse **Siguiente**. De forma predeterminada, el Agente de Siebel supervisa los registros de componentes de la Tabla 212 en la página 811. Para añadir hasta 10 registros de componentes adicionales a la supervisión, especifique el alias de componente correspondiente; por ejemplo, `SCBroker`.

   Consulte la sección Tabla 210 en la página 810 para obtener una descripción de cada uno de los parámetros de configuración.

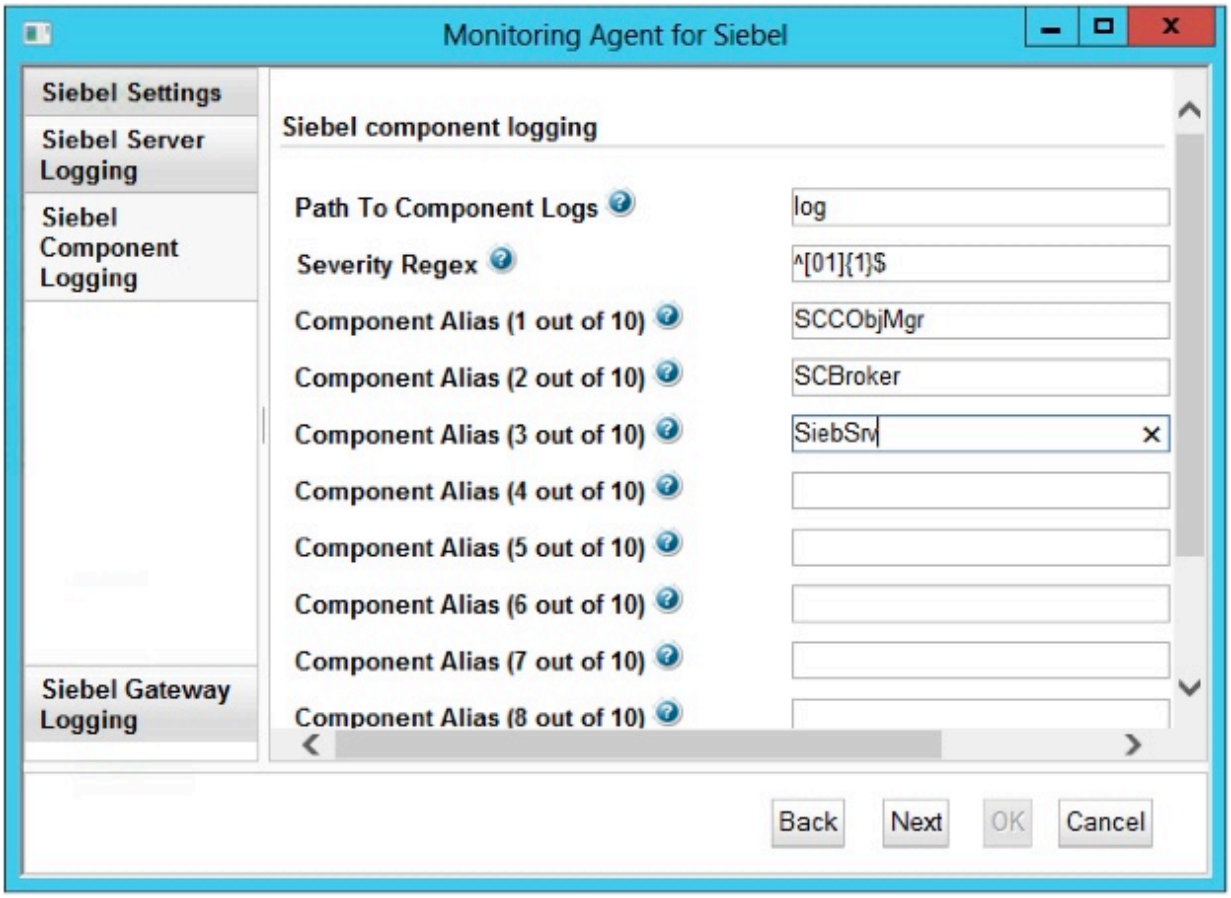


Figura 25. La ventana para especificar registros de componente adicionales que desee supervisar.

7. Opcional: Edite los valores de registro de pasarela de Siebel.

   Consulte la sección Tabla 211 en la página 810 para obtener una descripción de cada uno de los parámetros de configuración.

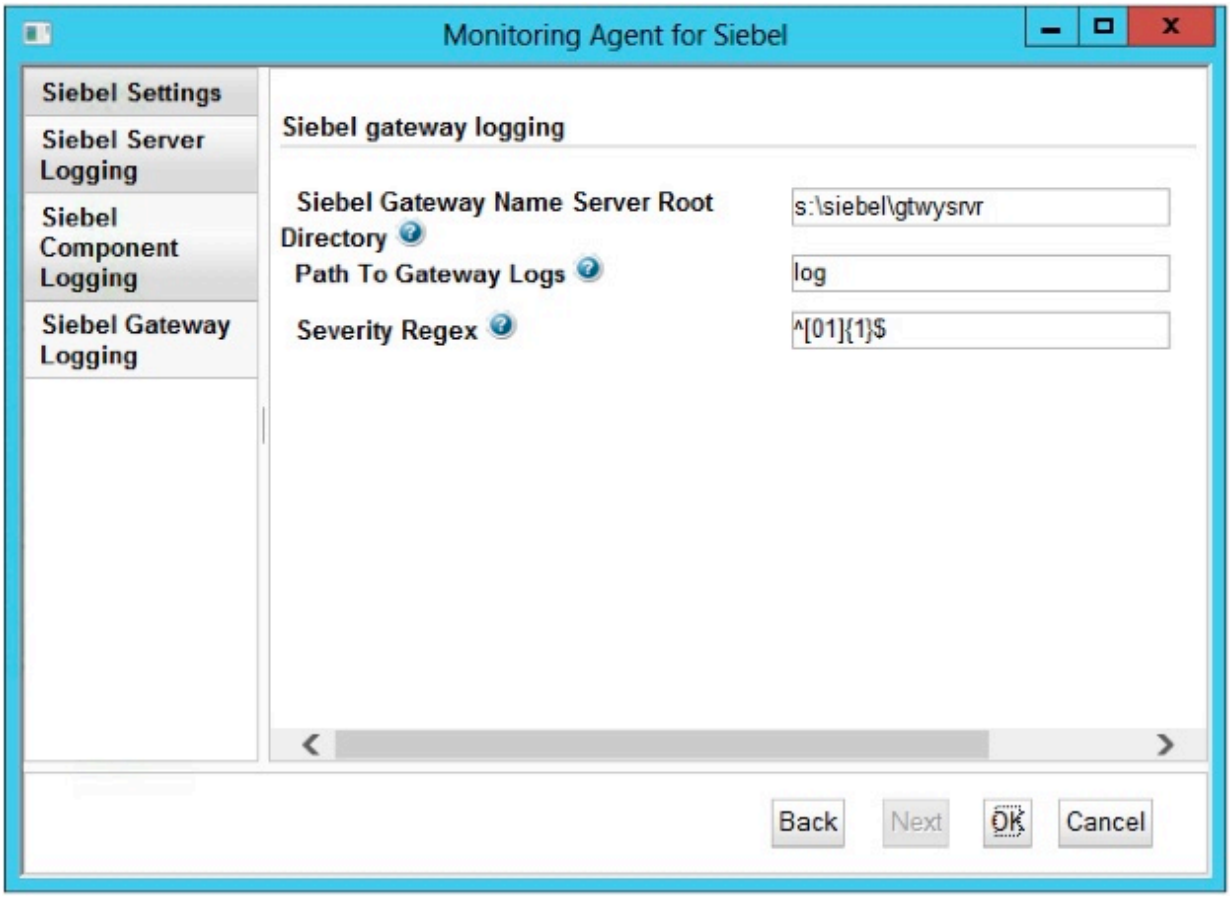


Figura 26. La ventana para especificar valores de registro de pasarela de Siebel.

8. Pulse **Aceptar** para completar la configuración.
9. En la ventana de IBM Cloud Application Performance Management, pulse con el botón derecho del ratón la instancia que ha configurado y luego pulse **Iniciar**.

Configuración del agente respondiendo a solicitudes

Después de la instalación del Agente de Siebel, debe configurarlo para poder iniciar el agente. Si el Agente de Siebel está instalado en un sistema Linux o UNIX local, puede seguir estas instrucciones para configurarlo interactivamente a través de solicitudes de línea de mandatos.

Acerca de esta tarea

Recuerde: Si está volviendo a configurar una instancia de agente configurada, se visualiza el valor que se establece en la última configuración para cada opción. Si desea borrar un valor existente, pulse la tecla de espacio cuando se visualice el valor.

Procedimiento

- Siga estos pasos para configurar el Agente de Siebel ejecutando un script y respondiendo a solicitudes.
  a) En la línea de mandatos, ejecute el mandato siguiente:

  dir_instalación/bin/siebel-agent.sh config **nombre_instancia**

  Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

  Ejemplo

  ```
  /opt/ibm/apm/agent/bin/siebel-agent.sh config example-inst01
  ```

b) Responda a las solicitudes para establecer valores de configuración para el agente.

Consulte la sección "Parámetros de configuración para el Agente de Siebel" en la página 808 para obtener una descripción de cada uno de los parámetros de configuración.

c) Ejecute el mandato siguiente para iniciar el agente:

dir_instalación/bin/siebel-agent.sh start **nombre_instancia**

Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

Ejemplo

```
/opt/ibm/apm/agent/bin/siebel-agent.sh start example-inst01
```

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

- Para configurar el Agente de Siebel en modalidad silenciosa, realice los pasos siguientes:
  a) En un editor de texto, abra el archivo `siebel_silent_config.txt` que está disponible en la siguiente vía de acceso:
     – Linux AIX *dir_instalación*/samples/siebel_silent_config.txt
     – Windows *dir_instalación*\samples\siebel_silent_config.txt

     Donde *dir_instalación* es la vía de acceso donde está instalado el agente.

     Ejemplo

     – Linux AIX /opt/ibm/apm/agent/samples/siebel_silent_config.txt
     – Windows C:\IBM\APM\samples\siebel_silent_config.txt

  b) En el archivo `siebel_silent_config.txt`, especifique valores para todos los parámetros obligatorios. También puede modificar los valores predeterminados de otros parámetros.

     Consulte la sección "Parámetros de configuración para el Agente de Siebel" en la página 808 para obtener una descripción de cada uno de los parámetros de configuración.

  c) Guarde y cierre el archivo `siebel_silent_config.txt` y ejecute el mandato siguiente:
     – Linux AIX *dir_instalación*/bin/siebel-agent.sh config **nombre_instancia** *dir_instalación*/samples/siebel_silent_config.txt
     – Windows *dir_instalación*\bin\siebel-agent.bat config **nombre_instancia** *dir_instalación*\samples\siebel_silent_config.txt

     Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

Importante: Asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

Ejemplo

- Linux AIX `/opt/ibm/apm/agent/bin/siebel-agent.sh config example-inst01 /opt/ibm/apm/agent/samples/siebel_silent_config.txt`
- Windows `C:\IBM\APM\bin\ siebel-agent.bat config example-inst01 C:\IBM\APM\samples\siebel_silent_config.txt`

d) Ejecute el mandato siguiente para iniciar el agente:

- Linux AIX *dir_instalación*`/bin/siebel-agent.sh start` **nombre_instancia**
- Windows *dir_instalación*`\bin\siebel-agent.bat start` **nombre_instancia**

Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

Ejemplo

- Linux AIX `/opt/ibm/apm/agent/bin/siebel-agent.sh start example-inst01`
- Windows `C:\IBM\APM\bin\siebel-agent.bat start example-inst01`

Parámetros de configuración para el Agente de Siebel

Los parámetros de configuración para el Agente de Siebel se visualizan en tablas que los agrupan por categorías.

1. Valores de Siebel - Valores genéricos de entorno Siebel.
2. Registro de servidor Siebel - valores específicos para supervisar registros del servidor Siebel.
3. Registro de componentes de Siebel - Valores específicos para supervisar una lista personalizada de registros de componentes de Siebel.
4. Registro de pasarela de Siebel - Valores específicos para supervisar registros de pasarela de Siebel.

Tabla 208. Valores de Siebel

Nombre de parámetro	Descripción	Necesario para opción de tipo de servidor	Nombre de parámetro del archivo de configuración silenciosa
Tipo(s) de servidor	Indica los tipos de servidor que están instalados en el sistema local.	• **Sólo servidor de pasarela** • **Sólo servidor Siebel** • **Servidor Siebel y servidor de pasarela**	**KUY_SERVER_TYPE**
Nombre de la empresa	El nombre de la empresa de Siebel.	• **Sólo servidor Siebel** • **Servidor Siebel y servidor de pasarela**	**KUY_ENTERPRISE**

Tabla 208. Valores de Siebel (continuación)

Nombre de parámetro	Descripción	Necesario para opción de tipo de servidor	Nombre de parámetro del archivo de configuración silenciosa
Nombre de servidor Siebel	Nombre del servidor Siebel que se va a supervisar. **Nota:** este no es el nombre de host del servidor. Es el nombre del servidor que se utiliza al ejecutar el mandato **srvrmgr** de Siebel.	• **Sólo servidor Siebel** • **Servidor Siebel y servidor de pasarela**	**KUY_SERVER**
Nombre de pasarela de Siebel	El servidor de nombres de pasarela de Siebel para supervisar y, opcionalmente, el puerto, por ejemplo `gtwysrvr` o `gtwysrvr:1234`.	• **Sólo servidor Siebel** • **Servidor Siebel y servidor de pasarela**	**KUY_GATEWAY**
Directorio raíz de servidor Siebel	Directorio de instalación base del servidor de aplicaciones Siebel.	• **Sólo servidor Siebel** • **Servidor Siebel y servidor de pasarela**	**KUY_INSTALL_ROOT**
ID de administrador de Siebel	El ID de usuario específico de Siebel que agente utilizará para autenticarse en la empresa de Siebel al ejecutar el mandato **srvrmgr**. Por ejemplo: `SADMIN`	• **Sólo servidor Siebel** • **Servidor Siebel y servidor de pasarela**	**KUY_ADMIN_ID**
Contraseña de administrador de Siebel	La contraseña del administrador del servidor Siebel.	• **Sólo servidor Siebel** • **Servidor Siebel y servidor de pasarela**	**KUY_ADMIN_PASSWORD**

Tabla 209. Valores de registro de servidor Siebel

Nombre de parámetro	Descripción	Nombre de parámetro del archivo de configuración silenciosa
Vía de acceso a registros de servidor	La vía de acceso relativa desde el "Directorio raíz de servidor Siebel" a los registros. Para inhabilitar la captura de registros del servidor Siebel, especifique una vía de acceso no válida. Por ejemplo: `xyz`.	**KUY_SERVER_LOGGING_PATH**

Tabla 209. Valores de registro de servidor Siebel (continuación)		
Nombre de parámetro	**Descripción**	**Nombre de parámetro del archivo de configuración silenciosa**
Expresión regular de gravedad	La expresión regular utilizada para capturar registros del servidor Siebel coincidentes con un nivel de gravedad. El uso del valor predeterminado `^[01]{1}$` facilita la captura de errores de nivel 0 y 1.	**KUY_SERVER_LOGGING_SEVERITY_REGEX**

Tabla 210. Valores de registro de componentes de Siebel		
Nombre de parámetro	**Descripción**	**Nombre de parámetro del archivo de configuración silenciosa**
Vía de acceso a registros de componente	La vía de acceso relativa desde el "Directorio raíz de servidor Siebel" a los registros. Para inhabilitar la captura de registros del servidor Siebel, especifique una vía de acceso no válida. Por ejemplo: `xyz`.	**KUY_COMPONENT_LOGGING_PATH**
Expresión regular de gravedad	La expresión regular utilizada para capturar registros del servidor Siebel coincidentes con un nivel de gravedad. El uso del valor predeterminado `^[01]{1}$` facilita la captura de errores de nivel 0 y 1.	**KUY_COMPONENT_LOGGING_SEVERITY_ REGEX**
Alias de componente (*N* de 10)	El alias de componente para el que debe supervisarse un registro de componente adicional. Ejemplo: `SCBroker`. Donde *N* representa de 1 a 10 componentes opcionales.	**KUY_CUSTCOMPLOG_00** a **KUY_CUSTCOMPLOG_09**

Tabla 211. Valores de registro de pasarela de Siebel		
Nombre de parámetro	**Descripción**	**Nombre de parámetro del archivo de configuración silenciosa**
Directorio raíz de servidor de nombres de pasarela de Siebel	Directorio de instalación base del servidor de nombres de pasarela de Siebel.	**KUY_GATEWAY_ROOT**

Tabla 211. Valores de registro de pasarela de Siebel (continuación)		
Nombre de parámetro	**Descripción**	**Nombre de parámetro del archivo de configuración silenciosa**
Vía de acceso a registros de pasarela	La vía de acceso relativa desde el directorio raíz de servidor de nombres de pasarela de Siebel a los registros de pasarela. Para inhabilitar la captura de registros de servidor de nombres de pasarela, especifique una vía de acceso no válida. Por ejemplo: `xyz`.	**KUY_GW_LOGGING_PATH**
Expresión regular de gravedad	La expresión regular utilizada para capturar registros del servidor Siebel coincidentes con un nivel de gravedad. El uso del valor predeterminado `^[01]{1}$` facilita la captura de errores de nivel 0 y 1.	**KUY_GW_LOGGING_SEVERITY_REGEX**

Registros de componentes de Siebel que siempre se supervisan

Los registros de 10 componentes de Siebel siempre se supervisan.

Tabla 212. Alias y nombres de componentes de Siebel para los que siempre se supervisan los registros de componente.	
Alias de componente	**Nombre de componente**
SCCObjMgr	Call Center Object Manager
SMObjMgr	Marketing Object Manager
SSEObjMgr	Sales Object Manager
CommInboundRcvr	Communications Inbound Receiver
CommOutboundMg	Communications Outbound Manager
CommSessionMgr	Communications Session Manager
WorkMon	Workflow Monitor Agent
WfProcBatchMgr	Workflow Process Batch Manager
WfProcMgr	Workflow Process Manager
SiebSrvr	Siebel Server

Configuración de la supervisión de Sterling Connect Direct

Debe configurar el Agente de Sterling Connect Direct de forma que el agente pueda recopilar datos de los servidores de Connect Direct para supervisar las estadísticas de transferencia de archivos y de estado de los servidores de Connect Direct.

Antes de empezar

Revise los requisitos previos de hardware y software, consulte Informes de compatibilidad de productos de software para el agente de Sterling Connect Direct

Acerca de esta tarea

- Para configurar el agente en sistemas Windows, puede utilizar la ventana IBM Cloud Application Performance Management o el archivo de respuestas silencioso.
- Para configurar el agente en sistemas Linux, puede ejecutar el script y responder a las solicitudes, o utilizar el archivo de respuestas silencioso.

Configuración del agente en sistemas Windows

Puede utilizar la ventana de IBM Cloud Application Performance Management para configurar el agente en sistemas Windows.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en **Plantilla** en la columna **Tarea/Subsistema** y pulse **Configurar agente**.
3. En el campo **Especificar un nombre de instancia exclusivo**, escriba el nombre de una instancia del agente y pulse **Aceptar**.

   Nota: Limite la longitud del nombre de instancia de agente. Es preferible que sea entre 7 y 10 caracteres.
4. En la ventana **Monitoring Agent for Sterling Connect Direct**, en la pestaña **Detalles del servidor de Connect Direct** especifique los valores de los parámetros de configuración y pulse **Aceptar**.

   Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 813.
5. Pulse **Siguiente**.
6. En la pestaña Parámetros Java, conserve los valores predeterminados y pulse **Siguiente**.
7. En la pestaña Configuración del cliente de la API de Java, pulse **Aceptar**.
8. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la instancia del agente que ha creado y pulse **Inicio** para iniciar el agente.

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información acerca de cómo usar la consola, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente en sistemas Linux

Para configurar el agente en sistemas operativos Linux, debe ejecutar el script y responder a las solicitudes.

Procedimiento

1. En la línea de mandatos, cambie la vía de acceso al directorio de instalación de agente. Ejemplo: `/opt/ibm/apm/agent/bin`
2. Ejecute el mandato **`/sterling_connect_direct-agent.sh config nombre_instancia`**.

   Nota: El *nombre_instancia* es el nombre que desea proporcionar a la instancia del agente.
3. La línea de mandato muestra el mensaje `¿Desea editar "Monitoring Agent for Sterling Connect Direct"? [1=Sí, 2=No]`.
4. Escriba 1 para editar los valores.

5. Especifique valores para los parámetros de configuración cuando se le solicite. Para obtener más información sobre los parámetros de configuración, consulte "Parámetros de configuración del agente" en la página 813.
6. Ejecute el mandato para iniciar el agente **./sterling_connect_direct-agent.sh start nombre_instancia**

Qué hacer a continuación

Inicie la sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Obtenga más información sobre cómo utilizar la Consola de Cloud APM, en el apartado "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

Puede utilizar el archivo de respuestas silencioso para configurar el Monitoring Agent for Sterling Connect Direct en sistemas Linux y Windows. Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

1. Abra el archivo de respuestas silencioso de *dir_instalación*/samples/sterling_connect_direct_silent_config.txt en un editor de texto.
2. Escriba el nombre del servidor, el nombre del usuario, la contraseña y el directorio de instalación en el archivo y guárdelo.
3. En el indicador de mandatos, vaya a *dir_instalación*/bin y ejecute el mandato

   Linux AIX ./sterling_connect_direct-agent.sh config <nombre_instancia> *dir_instalación*/samples/sterling_connect_direct_silent_config.txt.

   Windows ./sterling_connect_direct-agent.bat config <nombre_instancia> *dir_instalación*/samples/sterling_connect_direct_silent_config.txt.

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Para obtener ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.

Parámetros de configuración del agente

Al configurar Monitoring Agent for Sterling Connect Direct puede establecer los valores para los parámetros de configuración.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del Monitoring Agent for Sterling Connect Direct.

Tabla 213. Nombres y descripciones de los parámetros de configuración		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Nombre de instancia	El valor predeterminado para este campo es igual que el valor que se especifica en el campo **Especificar un nombre de instancia exclusivo**.	Sí
Nombre de servidor	El nombre de host o la dirección IP del servidor de Sterling Connect Direct.	Sí
Puerto de servidor	El puerto del servidor de Sterling Connect Direct. El valor predeterminado para Sterling Connect Direct es 1363.	Sí
Nombre de usuario	El nombre de usuario para conectarse al servidor de Sterling Connect Direct.	Sí
Contraseña	La contraseña para conectarse al servidor de Sterling Connect Direct.	Sí
Directorio de inicio de Java	La vía de acceso a la carpeta en la que está instalado Java.	No
Nivel de rastreo de Java	El nivel de rastreo que utilizan los proveedores de Java. El valor predeterminado para Sterling Connect Direct es Error	Sí
Argumentos de JVM	Este parámetro permite especificar una lista opcional de argumentos para la Java Virtual Machine.	No
Vía de acceso de clases para los jar externos	La vía de acceso para los jar que necesita el proveedor de datos de la API de Java que no se incluyen con el agente.	No

Configuración de la supervisión de Sterling File Gateway

El Monitoring Agent for Sterling File Gateway supervisa la aplicación IBM Sterling File Gateway utilizando las API REST de B2B (business-to-business) y la base de datos de pasarela. Debe configurar el Agente de Sterling File Gateway de forma que el agente pueda recopilar datos de los orígenes de datos y supervisar las estadísticas y el estado de la aplicación Sterling File Gateway. Puede configurar el agente en sistemas Windows y Linux.

Antes de empezar

- Revise los requisitos previos de hardware y software, consulte Informes de compatibilidad de productos de software para el agente de Sterling File Gateway.
- Asegúrese de que las API REST de B2B estén instaladas en su nodo de pasarela de archivos. Para obtener más información sobre la instalación de la API REST de B2B, consulte “Instalación de la API REST de B2B” en la página 815.

Acerca de esta tarea

El Agente de Sterling File Gateway es un agente de varias instancias. Deberá crear la primera instancia e iniciar el agente manualmente.

- Para configurar el agente en sistemas Windows, puede utilizar la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
- Para configurar el agente en sistemas Linux, puede ejecutar el script y responder a las solicitudes, o utilizar el archivo de respuestas silencioso.

Instalación de la API REST de B2B

Puede instalar y configurar las API REST B2B (business-to-business) en el nodo de Sterling File Gateway. Las API REST de B2B están disponibles en el instalador de B2B Integrator (V5.2.6.2).

Procedimiento

1. Vaya al directorio `<dir_instalación>/bin`.

   Siendo *dir_instalación* el directorio del instalador del agente para el integrador de B2B.
2. Ejecute el mandato siguiente:

   - Linux `./InstallService.sh/dir_instalación/bin/b2bAPIs_10000602.jar`

     Donde *<dir_instalación>* es la ubicación en la que ha extraído el contenido del archivo multimedia.
   - Windows `./InstallService.cmd/dir_instalación/bin/b2bAPIs_10000602.jar`

     Donde *<dir_instalación>* es la carpeta del instalador de B2B.

Configuración del Agente de Sterling File Gateway en sistemas Windows

Puede configurar el Agente de Sterling File Gateway en los sistemas operativos Windows utilizando la ventana **IBM Cloud Application Performance Management**. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Acerca de esta tarea

El Agente de Sterling File Gateway proporciona valores predeterminados para algunos parámetros. Puede especificar diferentes valores para estos parámetros.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Monitoring Agent for Sterling File Gateway** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar el agente por primera vez, la opción **Configurar el agente** ya no estará disponible. Para configurar el agente de nuevo, pulse **Reconfigurar**.
3. En la ventana Agente de Sterling File Gateway , realice los pasos siguientes:
   a) Escriba un nombre exclusivo para la instancia del Agente de Sterling File Gateway y pulse **Aceptar**.
   b) En la pestaña **Detalles de la API de B2B**, especifique los valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.
   c) En la pestaña **Detalles de base de datos**, especifique los valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.
   d) En la pestaña **API de Java**, especifique los valores para los parámetros de configuración y, a continuación, pulse **Aceptar**.

   Para obtener más información sobre los parámetros de configuración de cada pestaña de la ventana Agente de Sterling File Gateway , consulte los temas siguientes:

   - "Parámetros de configuración para los detalles de la API de B2B" en la página 819
   - "Parámetros de configuración para los detalles de base de datos" en la página 820
   - "Parámetros de configuración para la API de Java" en la página 820
4. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Agente de Sterling File Gateway** y luego pulse **Iniciar**.

Configuración del Agente de Sterling File Gateway en sistemas Linux

Puede ejecutar el script de configuración para responder a solicitudes con el fin de configurar el Agente de Sterling File Gateway en los sistemas operativos Linux.

Procedimiento

1. Vaya a la línea de mandatos y ejecute el mandato **<dir_instalación>/bin/ sterling_file_gateway-agent.sh config nombre_instancia**.

   Siendo *nombre_instancia* el nombre que desea conceder a la instancia y *dir_instalación* es la vía de acceso al directorio de instalación del agente.
2. Se le solicitará que proporcione valores para todos los parámetros de configuración obligatorios. Puede modificar los valores predeterminados de los parámetros de configuración.

   Para obtener más información sobre los parámetros de configuración, consulte los temas siguientes:

   - "Parámetros de configuración para los detalles de la API de B2B" en la página 819
   - "Parámetros de configuración para los detalles de base de datos" en la página 820
   - "Parámetros de configuración para la API de Java" en la página 820
3. Para iniciar el agente, ejecute el mandato **<dir_instalación>/bin/sterling_file_gateway-agent.sh start nombre_instancia**.

Configuración del Agente de Sterling File Gateway utilizando el archivo de respuestas silencioso.

Puede utilizar el archivo de respuestas silencioso para configurar el Agente de Sterling File Gateway sin responder a las solicitudes cuando ejecuta el script de configuración. Puede configurar el agente que utiliza el archivo de respuestas silencioso en ambos sistemas Windows y Linux. El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

- Para configurar el Agente de Sterling File Gateway en modalidad silenciosa, realice los pasos siguientes:
  a) En un editor de texto, abra el archivo `sterling_file_gatway_silent_config.txt`, que está disponible en la siguiente vía de acceso:
     – Linux *dir_instalación*`/samples/sterling_file_gatway_silent_config.txt`

       Ejemplo: **/opt/ibm/apm/agent/samples/ sterling_file_gateway_silent_config.txt**
     – Windows *dir_instalación*`\samples\sterling_file_gateway_silent_config.txt`

       Ejemplo **C:\IBM\APM\samples\sterling_file_gateway_silent_config.txt**
  b) En el archivo `sterling_file_gateway_silent_config.txt`, especifique valores para todos los parámetros obligatorios. También puede modificar los valores predeterminados de otros parámetros.

     Para obtener más información sobre los parámetros de configuración, consulte los temas siguientes:

     – "Parámetros de configuración para los detalles de la API de B2B" en la página 819
     – "Parámetros de configuración para los detalles de base de datos" en la página 820

– "Parámetros de configuración para la API de Java" en la página 820

c) Guarde y cierre el archivo `sterling_file_gateway_silent_config.txt` y ejecute el mandato siguiente:

– Linux *dir_instalación*/bin/sterling_file_gateway-agent.sh config *nombre_instancia* *dir_instalación*/samples/sterling_file_gateway_silent_config.txt

Ejemplo: **/opt/ibm/apm/agent/bin/sterling_file_gateway-agent.sh config nombre_instancia /opt/ibm/apm/agent/samples/sterling_file_gateway_silent_config.txt**

– Windows *dir_instalación*/bin/sterling_file_gateway-agent.bat config *nombre_instancia* *dir_instalación*/samples/sterling_file_gateway_silent_config.txt

Ejemplo **C:\IBM\APM\bin\sterling_file_gateway-agent.bat config nombre_instancia C:\IBM\APM\samples\sterling_file_gateway_silent_config.txt**

Siendo *nombre_instancia* el nombre que desea dar a la instancia y *dir_instalación* es la vía de acceso donde se ha instalado el agente.

Importante: Asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

d) Ejecute el mandato siguiente para iniciar el agente:

– Linux *dir_instalación*/bin/sterling_file_gateway-agent.sh start *nombre_instancia*

Ejemplo **/opt/ibm/apm/agent/bin/sterling_file_gateway-agent.sh start nombre_instancia**

– Windows *dir_instalación*\bin\sterling_file_gateway-agent.bat start *nombre_instancia*

Ejemplo **C:\IBM\APM\bin\sterling_file_gateway-agent.bat start nombre_instancia**

Configuración de variables de entono de agente para el proveedor de datos en Linux

Puede configurar las variables de entorno de Agente de Sterling File Gateway para el proveedor de datos en los sistemas operativos Linux.

Acerca de esta tarea

El Agente de Sterling File Gateway proporciona las variables de entorno que puede configurar para el proveedor de datos.

Procedimiento

1. Vaya al directorio <dir_instalación>/agent/config.
2. Abra el archivo `.fg.environment` en un editor y edite las variables de entorno.

   Para obtener más información acerca de las variables de entorno que puede configurar, consulte "Variables de entorno para el proveedor de datos" en la página 818.

Configuración de variables de entono de agente para el proveedor de datos en Windows

Puede configurar las variables de entorno del Agente de Sterling File Gateway para el proveedor de datos en sistemas operativos Windows utilizando la ventana **IBM Performance Management**.

Acerca de esta tarea

El Agente de Sterling File Gateway proporciona las variables de entorno que puede configurar para el proveedor de datos.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la instancia del agente y pulse **Avanzado** > **Editar archivo ENV** y edite los valores predeterminado de las variables de entorno.

   Para obtener más información acerca de las variables de entorno que puede configurar, consulte "Variables de entorno para el proveedor de datos" en la página 818.

Variables de entorno para el proveedor de datos

Tras configurar el Agente de Sterling File Gateway , puede modificar algunos valores de duración del umbral relacionados con la recopilación de datos de agente. Puede especificar estos valores en el archivo de entorno de agente.

La tabla siguiente contiene una descripción detallada de las variables de entorno para el proveedor de datos.

Tabla 214. Nombre y descripción de las variables de entorno para el proveedor de datos

Nombre de parámetro	**Descripción**
Duración de la recopilación para las transferencias de archivos (en horas) (**KFG_FILE_ARRIVED_INTERVAL**)	La duración en horas en que el agente recopila datos para las transferencias de archivos. El valor predeterminado es de 24 horas.
Intervalos de recopilación para actividades de transferencia de archivos que se visualizan como un diagrama de líneas (en horas) (**KFG_FILE_ACTIVITY_INTERVAL**)	La duración en horas en que el agente recopila datos para las actividades de transferencia de archivos. El valor predeterminado es de 1 hora. Por ejemplo, el agente recopila las actividades de transferencia de archivos que se han producido en la última hora. Estos datos serán visible en forma de diagramas de líneas en la página de la instancia. El valor predeterminado es de 1 hora.
Intervalo de umbral para socios inactivos (en días) (**KFG_INACTIVE_PARTNERS_INTERVAL**)	La duración de umbral en que un socio está inactivo o no ha recibido ni subido ningún archivo. El valor predeterminado es 10 días. Por ejemplo, si algún socio que no recibe ni transfiere ningún archivo los últimos 10 días, aparece como "Inactivo" en el agente.
Número máximo de archivos de registro del proveedor de datos (**KFG_LOG_FILE_MAX_COUNT**)	El número máximo de archivos de registro que el proveedor de datos crea antes de grabar encima de los archivos de registro anteriores. El valor predeterminado es 10.
Tamaño máximo en KB de cada inicio de sesión del proveedor de datos (**KFG_LOG_FILE_MAX_SIZE**)	El tamaño máximo en KB que debe alcanzar un archivo de registro del proveedor de datos antes de que el proveedor de datos cree un archivo de registro nuevo. El valor predeterminado es 5190 KB.

Tabla 214. Nombre y descripción de las variables de entorno para el proveedor de datos (continuación)	
Nombre de parámetro	**Descripción**
Nivel de detalle en el registro del proveedor de datos (**KFG_LOG_LEVEL**)	El nivel de detalles que se incluyen en el archivo de registro que crea el proveedor de datos. El valor predeterminado es 4 (Info). Los valores siguientes son válidos: • 1 (Desactivado): no se registra ningún mensaje. • 2 (Grave): sólo se registran los errores. • 3 (Aviso): todos los errores y mensajes que se registran en el nivel Grave y los errores potenciales que pueden provocar un comportamiento indeseable. • 4 (Info): todos los errores y mensajes que se registran en el nivel Aviso y los mensajes informativos de alto nivel que describen el estado del proveedor de datos cuando se procesa. • 5 (Bueno): todos los errores y mensajes que se registran en el nivel de información y los mensajes informativos de bajo nivel que describen el estado del proveedor de datos cuando se procesa. • 6 (Mejor): todos los errores y mensajes que se registran en el nivel Bueno y los mensajes informativos muy detallados, como por ejemplo la información de perfilado de rendimiento y datos de depuración. Si selecciona esta opción, el rendimiento del agente de supervisión puede verse perjudicado. Este valor está concebido para utilizarlo como herramienta para la determinación de problemas en colaboración con el personal de soporte de IBM. • 7 (El mejor): todos los errores y mensajes que se registran en el nivel Bueno y los mensajes informativos más detallados que incluyen datos y mensajes de programación de bajo nivel. Si selecciona esta opción, el rendimiento del agente de supervisión puede verse perjudicado. Este valor está concebido para utilizarlo como herramienta para la determinación de problemas en colaboración con el personal de soporte de IBM. • 8 (Todos): se registran todos los mensajes.
Captación de sucesos para todas las transferencias de archivos (**KFG_ALL_FGEVENTS**)	El distintivo para captar sucesos para todas las transferencias de archivos. Los valores válidos son Sí o No. El valor predeterminado es No. Si el valor se establece en No, el agente capta sucesos para transferencias de archivo fallidas para una duración configurable por el usuario. Si el valor se establece en Sí, el agente capta todos los sucesos para todas las transferencias de archivo para una duración configurable por el usuario.

Parámetros de configuración para los detalles de la API de B2B

Cuando configure el Agente de Sterling File Gateway , debe especificar los valores de los parámetros de configuración para los detalles de la API B2B (business-to-business).

La tabla siguiente contiene una descripción detallada de los parámetros de configuración para los detalles de la API B2B.

Tabla 215. Nombre y descripción de los parámetros de configuración para los detalles de la API B2B	
Nombre de parámetro	**Descripción**
Nombre de instancia (**nombre_instancia_KFG**)	El nombre de la instancia. **Restricción:** El campo Nombre de instancia muestra el nombre de la instancia que especifica al configurar el agente por primera vez. Al volver a configurar el agente, no puede cambiar el nombre de instancia del agente.
Nombre de servidor (**KFG_API_SERVICES_Node_ADDRESS**)	El nombre de host o la dirección IP del servicio de la API B2B.
Puerto de servidor (**KFG_API_SERVICES_PORT**)	El puerto de la API B2B.
Nombre de usuario (**KFG_API_SERVICES_USERNAME**)	Un nombre de usuario que va a conectar al servicio de la API B2B.
Contraseña (**KFG_API_SERVICES_PASSWORD**)	La contraseña del nombre de usuario que utiliza para conectarse al servicio de la API B2B.

Parámetros de configuración para los detalles de base de datos

Cuando configure el Agente de Sterling File Gateway , debe especificar los valores de los parámetros de configuración para los detalles de bases de datos.

La tabla siguiente contiene una descripción detallada de los parámetros de configuración para los detalles de bases de datos.

Tabla 216. Nombre y descripción de los parámetros de configuración para los detalles de bases de datos	
Nombre de parámetro	**Descripción**
Nombre del servidor de base de datos (**KFG_DB_Node_ADDRESS**)	El nombre de host o la dirección IP del servidor de base de datos de Sterling File Gateway.
Usuario de base de datos (**KFG_DB_USERNAME**)	El nombre del usuario de la base de datos.
Contraseña de base de datos (**KFG_DB_PASSWORD**)	La contraseña de la base de datos.
Puerto de base de datos (**KFG_DB_PORT**)	El puerto de la base de datos.
Tipo de base de datos (**KFG_DB_TYPE**)	El tipo de la base de datos.

Parámetros de configuración para la API de Java

Cuando configure el Agente de Sterling File Gateway , debe especificar valores de los parámetros de configuración para la API de Java.

La tabla siguiente contiene una descripción detallada de los parámetros de configuración para la API de Java.

Tabla 217. Nombre y descripción de los parámetros de configuración para la API de Java	
Nombre de parámetro	**Descripción**
Vía de acceso de clases para archivos JAR externos (**KFG_CLASSPATH**)	La vía de acceso de archivo JAR del controlador de bases de datos que desea especificar para la base de datos correspondiente.

Configuración de la supervisión del servidor Sybase

El Agente de Sybase ofrece un punto central de gestión de las bases de datos distribuidas. Recopila la información necesaria para que los administradores del sistema y de la base de datos puedan examinar el rendimiento del sistema del servidor Sybase, detectar problemas con antelación y evitarlos. Los administradores del sistema y de la base de datos pueden establecer los niveles de umbral y marcadores necesarios para que se desencadenen alertas cuando el sistema alcance estos umbrales.
Debe configurar Monitoring Agent for Sybase Server para supervisar el servidor Sybase.

Antes de empezar

Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Sybase.

Acerca de esta tarea

Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Agente de Sybase es un agente de varias instancias. Debe configurar e iniciar cada instancia de agente manualmente.

Procedimiento

1. Configure el agente de supervisión.
   - "Configuración del agente mediante la interfaz de línea de mandatos" en la página 823
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 824
2. Inicie y detenga el agente de supervisión mediante el mandato de agente **sybase-agent**.

   Para obtener más información sobre **sybase-agent**, consulte *Utilización de mandatos de agente* en https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.
3. Conecte el agente de supervisión al servidor de Performance Management mediante el mandato **agent2server**.

   Para obtener más información sobre **agent2server**, consulte *Utilización de mandatos de agente* en https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Concesión de permisos

Debe otorgar permisos al ID de usuario utilizado para supervisar el servidor Sybase.

Antes de empezar

Instale la Agente de Sybase.

Para otorgar permisos, debe tener el rol de administrador de base de datos.

Acerca de esta tarea

El ID de usuario que utiliza el agente de supervisión debe tener acceso a las tablas de Sybase y a las tablas de supervisor instaladas.

Puede realizar las tareas siguientes:

- Crear un ID de usuario para el agente de supervisor.
- Otorgar permiso al nuevo ID de usuario y a las tablas de supervisor instaladas.

Si no está ejecutando Agente de Sybase como usuario `root`, asegúrese de que el ID de usuario pertenece al grupo `Sybase` y que tiene acceso de lectura a los archivos de registro de Sybase.

Procedimiento

1. Especifique el mandato para el sistema operativo que está utilizando.
   - Windows

     ```
     cd dir_instalación\tmaitm6\SQLLIB
     ```

   - UNIX

     ```
     cd dir_instalación/misc
     ```

   Donde *dir_instalación* es el directorio de inicio en el que está instalado el servidor Sybase.
2. Utilice el mandato **`isql`** para iniciar la sesión en el servidor Sybase como usuario `sa`.
3. Ejecute el mandato siguiente para configurar el ID que utiliza el agente de Sybase para la comunicación con el servidor Sybase:

   ```
   1>sp_addlogin nombre_usuario, contraseña 2>g
   ```

   Donde:
   - *nombre_usuario* es el ID de usuario. De forma predeterminada, es `tivoli`.

     Si el ID de usuario no es `tivoli`, edite el archivo `koygrant.sql` y cambie `tivoli` por el ID de usuario correcto.
   - *contraseña* es la contraseña del usuario.

   Nota:

   Ubicación del archivo `koygrant.sql`:
   - Windows `\opt\ibm\apm\agent\misc\`
   - UNIX `/opt/ibm/apm/agent/misc/`
4. Ejecute el mandato siguiente para otorgar permiso a las tablas en la base de datos:

   ```
   isql -U sa -P contraseña -S nombre_servidor -i vía_acceso_archivo_koygrantkoygrant.sql
   ```

   Donde:
   - *contraseña* es la contraseña de usuario `sa`.
   - *nombre_servidor* es el nombre de servidor de bases de datos.
   - *vía_acceso_archivo_koygrant* se encuentra en la siguiente ubicación:

     Nota:

     – Windows `\opt\ibm\apm\agent\misc\`

     – UNIX `/opt/ibm/apm/agent/misc/`
5. Ejecute el mandato siguiente para crear tablas de proxy utilizadas para las tablas de supervisor instaladas:

   ```
   isql -U sa -P contraseña -S nombre_servidor
        -i $SYBASE/ASE-12_5/scripts/installmontables
   ```

   Donde:
   - *contraseña* es la contraseña de usuario `sa`.
   - *nombre_servidor* es el nombre de servidor de bases de datos.

Qué hacer a continuación

Cuando los permisos se han otorgado correctamente, puede configurar el agente de supervisión.

Configuración del agente mediante la interfaz de línea de mandatos

Puede configurar Monitoring Agent for Sybase Server mediante la interfaz de línea de mandatos.

Antes de empezar

Agente de Sybase no da soporte a la configuración remota. Por lo tanto, debe asegurarse de que el servidor Sybase esté instalado en el mismo host donde está instalado Agente de Sybase.

Agente de Sybase sólo da soporte a las versiones 15.7 y 16.0 del servidor Sybase.

Se crea el ID de usuario que se utiliza para conectar al servidor de bases de datos.

Acerca de esta tarea

Agente de Sybase es un agente de varias instancias. Debe configurar e iniciar cada instancia de agente manualmente.

Procedimiento

1. Ejecute el mandato siguiente para configurar el agente.
   - Windows

     ```
     dir_instalación\bin\sybase-agent.bat nombre_instancia
     ```

   - UNIX

     ```
     dir_instalación/bin/sybase-agent.sh nombre_instancia
     ```

   Donde:

   - *dir_instalación* es el directorio de instalación del agente.
   - *nombre_instancia* es el nombre de instancia del servidor Sybase.
2. Cuando se le solicite que proporcione valores para los parámetros siguientes, pulse Intro para aceptar el valor predeterminado o especifique un valor y pulse Intro.
   a) Para el parámetro `Directorio de inicio`, especifique la vía de acceso del directorio de inicio del servidor Sybase.
      - Windows

        El ejemplo de `Directorio de inicio` es `\opt\sybase`.
      - UNIX

        El ejemplo de `Directorio de inicio` es `/opt/sybase`.

   b) Para el parámetro `Directorio de ASE`, especifique la vía de acceso del servidor de bases de datos ASE.
      - Windows

        El ejemplo de `Directorio de ASE` es `\opt\sybase\ASE-12_5`.
      - UNIX

        El ejemplo de `Directorio de ASE` es `/opt/sybase/ASE-12_5`.

   c) Para el parámetro `Directorio de cliente abierto`, especifique la ubicación de instalación del cliente abierto de Sybase.
      - Windows

        El ejemplo de `Directorio del cliente abierto` es `\opt\sap\ocs-16_0`.

- UNIX

  El ejemplo de `Directorio de cliente abierto` es `/opt/sap/ocs-16_0`.

d) Para el parámetro `ID de usuario`, especifique el ID de usuario que utiliza el agente de supervisión para conectarse al servidor Sybase.

   El `ID DE USUARIO` predeterminado es `tivoli`.

e) Para el parámetro `CONTRASEÑA`, especifique la contraseña del ID de usuario que utiliza el agente de supervisión para conectarse al servidor Sybase.

f) Para el parámetro `VERSIÓN`, especifique la versión del servidor Sybase.

   Agente de Sybase sólo da soporte a las versiones 15.7 y 16.0 del servidor Sybase.

g) Para el parámetro `ARCHIVO DE REGISTRO DE ERRORES`, especifique el nombre de archivo completo del archivo de registro de errores para el servidor Sybase.

   - Windows

     El ejemplo de `ARCHIVO DE REGISTRO DE ERRORES` es `\opt\sap\ASE-16_0\install \`*`nombre_servidor`*`.log`.

   - UNIX

     El ejemplo de `ARCHIVO DE REGISTRO DE ERRORES` es `/opt/sap/ASE-16_0/install/`*`nombre_servidor`*`.log`.

   Donde *nombre_servidor* es el nombre de servidor Sybase.

h) Para el parámetro `AMPLIADO`, especifique el parámetro ampliado que utiliza el soporte para excluir determinadas ejecuciones del cursor. Opcionalmente, pulse Intro sin especificar ningún valor para ejecutar todos los cursores.

   Las opciones del parámetro `AMPLIADO` son `DBD2,DBD15,KOYSEGD`.

   - `DBD2` excluirá la ejecución del cursor para los conjuntos de datos Sybase_Database_Detail y Sybase_Database_Summary.
   - `DBD15` excluirá la ejecución del cursor para los conjunto de datos Sybase_Database_Detail.
   - `KOYSEGD` excluirá la ejecución del cursor para el conjunto de datos Sybase_Segment_Detail.

Qué hacer a continuación

Cuando se haya completado la configuración, puede iniciar el agente de supervisión y conectar el agente de supervisión al servidor de Performance Management.

Para iniciar Agente de Sybase, utilice el mandato `sybase-agent` del agente.

Para conectar Agente de Sybase al servidor de Performance Management, utilice el mandato `agent2server`.

Para obtener más información sobre `sybase-agent` y `agent2server`, consulte *Utilización de mandatos de agente* en https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Configuración del agente mediante el archivo de respuestas silencioso

Puede configurar Monitoring Agent for Sybase Server mediante el archivo de respuestas silencioso.

Antes de empezar

Agente de Sybase no da soporte a la configuración remota. Por lo tanto, debe asegurarse de que el servidor Sybase esté instalado en el mismo host donde está instalado Agente de Sybase.

Agente de Sybase sólo da soporte a las versiones 15.7 y 16.0 del servidor Sybase.

Se crea el ID de usuario que se utiliza para conectar al servidor de bases de datos.

Acerca de esta tarea

Agente de Sybase es un agente de varias instancias. Debe configurar e iniciar cada instancia de agente manualmente.

Debe editar el archivo de respuestas silencioso y ejecutar el mandato de agente para configurar el agente de supervisión.

Procedimiento

1. Edite el archivo de respuestas silencioso.
   - Windows

     El archivo de respuestas silencioso se encuentra en: *dir_instalación*\samples\sybase_silent_config.txt.
   - UNIX

     El archivo de respuestas silencioso se encuentra en: *dir_instalación*/samples/sybase_silent_config.txt.

   Donde *dir_instalación* es el directorio de instalación del agente.

   a) Para el parámetro Directorio de inicio, especifique la vía de acceso del directorio inicial del servidor Sybase.
      - Windows

        El ejemplo de Directorio de inicio es \opt\sybase.
      - UNIX

        El ejemplo de Directorio de inicio es /opt/sybase.

   b) Para el parámetro Directorio de ASE, especifique la vía de acceso del servidor de bases de datos ASE.
      - Windows

        El ejemplo de Directorio de ASE es \opt\sybase\ASE-12_5.
      - UNIX

        El ejemplo de Directorio de ASE es /opt/sybase/ASE-12_5.

   c) Para el parámetro Directorio de cliente abierto, especifique la ubicación de instalación del cliente abierto de Sybase.
      - Windows

        El ejemplo de Directorio del cliente abierto es \opt\sap\ocs-16_0.
      - UNIX

        El ejemplo de Directorio de cliente abierto es /opt/sap/ocs-16_0.

   d) Para el parámetro ID DE USUARIO, especifique el ID de usuario que utiliza el agente de supervisión para conectarse al servidor Sybase.

      El ID DE USUARIO predeterminado es tivoli.

   e) Para el parámetro CONTRASEÑA, especifique la contraseña del ID de usuario que utiliza el agente de supervisión para conectarse al servidor Sybase.

   f) Para el parámetro VERSIÓN, especifique la versión del servidor Sybase.

      Agente de Sybase sólo da soporte a las versiones 15.7 y 16.0 del servidor Sybase.

   g) Para el parámetro ARCHIVO DE REGISTRO DE ERRORES, especifique el nombre de archivo completo del archivo de registro de errores para el servidor Sybase.
      - Windows

El ejemplo de ARCHIVO DE REGISTRO DE ERRORES es \opt\sap\ASE-16_0\install *nombre_servidor*.log.

- UNIX

  El ejemplo de ARCHIVO DE REGISTRO DE ERRORES es /opt/sap/ASE-16_0/install/*nombre_servidor*.log.

Donde *nombre_servidor* es el nombre de servidor Sybase.

h) Para el parámetro AMPLIADO, especifique el parámetro ampliado que utiliza el soporte para excluir determinadas ejecuciones del cursor. De forma opcional, déjelo en blanco para ejecutar todos los cursores.

Las opciones de AMPLIADO son DBD2,DBD15,KOYSEGD.

- DBD2 excluirá la ejecución del cursor para los conjuntos de datos Sybase_Database_Detail y Sybase_Database_Summary.
- DBD15 excluirá la ejecución del cursor para los conjunto de datos Sybase_Database_Detail.
- KOYSEGD excluirá la ejecución del cursor para el conjunto de datos Sybase_Segment_Detail.

2. Guarde el archivo de respuestas silencioso.
3. Ejecute el mandato de agente siguiente para configurar el agente de supervisión.

- Windows

```
dir_instalación\bin\sybase-agent.bat config nombre_instancia
 dir_instalación\samples\sybase_silent_config.txt
```

- UNIX

```
dir_instalación/bin/sybase-agent.sh config nombre_instancia
 dir_instalación/samples/sybase_silent_config.txt
```

Donde:

- *dir_instalación* es el directorio de instalación del agente.
- *nombre_instancia* es el nombre de servidor Sybase.

Qué hacer a continuación

Cuando se haya completado la configuración, puede iniciar el agente de supervisión y conectar el agente de supervisión al servidor de Performance Management.

Para iniciar Agente de Sybase, utilice el mandato **sybase-agent**.

Para conectar Agente de Sybase al servidor de Performance Management, utilice el mandato **agent2server**.

Para obtener más información sobre **sybase-agent** y **agent2server**, consulte *Utilización de mandatos de agente* en https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Inhabilitación de lecturas incorrectas para consulta

El Agente de Sybase habilita de forma predeterminada las lecturas incorrectas para la ejecución de consultas para evitar el bloqueo.
Se utiliza la variable COLL_USE_NOLOCK para habilitar o inhabilitar las lecturas incorrectas de consulta.
Cuando las lecturas incorrectas están habilitadas, la consulta se ejecuta con el nivel de aislamiento cero para evitar el bloqueo.
Si desea inhabilitar las lecturas incorrectas para la consulta de agente, puede establecer la variable COLL_USE_NOLOCK en cero.

Antes de empezar

Para inhabilitar las `lecturas incorrectas` para la consulta de agente, asegúrese de que se ha instalado el agente.

Acerca de esta tarea

El Agente de Sybase habilita las `lecturas incorrectas` de forma predeterminada. Para inhabilitar las `lecturas incorrectas` para la consulta de agente, realice los pasos siguientes.

Procedimiento

1. Detenga el agente.
2. Establezca la variable `COLL_USE_NOLOCK` en cero.
   - UNIX
     a. Añada **`COLL_USE_NOLOCK=0`** al archivo *`INICIO_CANDLE`*`/config/.oy.environment`.
     b. Guarde los cambios y cierre el archivo.
   - Windows
     a. Localice el archivo de nombre de instancia *`INICIO_CANDLE`*`\TMAITM6_x64\KOYENV_`*`NOMBRE_INSTANCIA`*.
     b. Añada la línea siguiente al archivo.

        `COLL_USE_NOLOCK=0`

     c. Guarde los cambios y cierre el archivo.

   `INICIO_CANDLE` es el directorio de instalación de agente.
   `NOMBRE_INSTANCIA` es el nombre de instancia de agente.
3. Inicie el agente.

Configuración de la supervisión de Synthetic Playback

Debe configurar el Agente de Synthetic Playback para que el agente pueda recopilar datos sobre la disponibilidad y el rendimiento de las aplicaciones web internas. Estos datos se visualizan en Panel de instrumentos del rendimiento de aplicaciones.

Acerca de esta tarea

Configure el Agente de Synthetic Playback mediante la ejecución de un script y respondiendo a las solicitudes. A continuación, inicie el script y verifique que está en ejecución.

Importante: Sólo los usuarios existentes del complemento IBM Website Monitoring on Cloud pueden instalar, configurar y ejecutar el Agente de Synthetic Playback. Website Monitoring ha sido sustituido por IBM Cloud Availability Monitoring. Para obtener más información, consulte “Acerca de Availability Monitoring” en la página 1081.

Procedimiento

- Para configurar el agente mediante la ejecución del script y las respuestas a las solicitudes, siga estos pasos:
  a) Especifique *`dir_instalación`*`/bin/synthetic_playback-agent.sh config` donde *dir_instalación* es el directorio de instalación de Agente de Synthetic Playback.
  b) Cuando se le solicite `Editar agente de supervisión para los valores de reproducción sintética`, especifique 1 para continuar.
  c) Cuando se le solicite que especifique un nombre de centro de datos para el punto de presencia de reproducción, introduzca un nombre que identifique la ubicación de su agente.

Importante: Elija un nombre descriptivo para el punto de presencia de reproducción. Cuando haya completado la instalación del agente, puede seleccionar la ubicación por nombre como una ubicación de reproducción para las transacciones sintéticas y ver los datos de transacción de esa ubicación en Panel de instrumentos del rendimiento de aplicaciones.

d) Cuando se le solicite `Parámetros Java`, seleccione un `Nivel de rastreo Java`. Pulse Intro para elegir el parámetro por omisión o especifique un número del 1 al 8 para especificar un nivel de rastreo.

e) Cuando se le solicite `Vía de acceso de clase para jar externos`, pulse Intro para dejarlo en blanco o especifique la ubicación de un archivo jar externo.

- Para configurar el agente utilizando el archivo de respuestas silencioso, siga estos pasos:

  a) En un editor de texto, abra el archivo `synthetic_playback_silent_config.txt` que está disponible en la vía de acceso *dir_instalación*`/samples`.
  Por ejemplo:

  Linux `/opt/ibm/apm/agent/samples`

  b) En el archivo `synthetic_playback_silent_config.txt`, elimine el comentario y asigne valores a las propiedades siguientes:

  – Para `LOCATION`, asocie este parámetro al nombre del centro de datos o a un nombre que describa donde está instalado el agente.

  – Para `JAVA_TRACE_LEVEL`, asocie este parámetro a uno de los niveles de rastreo listados, por ejemplo, `JAVA_TRACE_LEVEL=ERROR`.

  Guarde el archivo.

  c) En la línea de mandatos, cambie la vía de acceso por *dir_instalación*`/bin`.

  d) Ejecute el siguiente mandato para configurar el agente en modalidad silenciosa:

```
synthetic_playback-agent.sh config dir_instalación/samples/
synthetic_playback_silent_config.txt
```

- Para iniciar el Agente de Synthetic Playback, escriba: *dir_instalación*`/bin/synthetic_playback-agent.sh start`.
- Para verificar que el Agente de Synthetic Playback está en ejecución, escriba: *dir_instalación*`/bin/synthetic_playback-agent.sh status`. Para obtener más información, consulte Tabla 12 en la página 187.

Qué hacer a continuación
Para ver el rendimiento de aplicaciones web internas, debe crear transacciones sintéticas en el Gestor de scripts sintéticos. Para obtener más información, consulte “Gestión de transacciones sintéticas y sucesos con Website Monitoring” en la página 1061.

Habilitación del soporte de proxy en sentido ascendente para el Agente de Synthetic Playback

Habilite el soporte de proxy en sentido ascendente para el Agente de Synthetic Playback para supervisar las solicitudes HTTP de las aplicaciones web internas a las aplicaciones web externas.

Antes de empezar
Asegúrese de que está ejecutando el Agente de Synthetic Playback versión 01.00.05.08 o posterior. Para comprobar qué versión de agente está ejecutando, entre *dir_instalación*`/bin/cinfo -t` en la línea de mandatos, donde *dir_instalación* es la ubicación de instalación del agente. Si está ejecutando cualquier otra versión del Agente de Synthetic Playback, debe descargar e instalar IBM Cloud Application Performance Management, Private 8.1.4.0 Agente de Synthetic Playback arreglo temporal 08 de IBM Fix Central (Especifique `Synthetic` en el campo **Search** y se visualizará la lista de arreglos temporales del Agente de Synthetic Playback). Para obtener instrucciones de instalación, consulte 8.1.4.0-IBM-IPM-SYNTHETIC-PLAYBACK-AGENT-IF0008 Readme.

Acerca de esta tarea

Las aplicaciones web internas detrás de un cortafuegos de empresa necesitan un proxy en sentido ascendente para acceder a los recursos web externos. Configure el valor de proxy del Agente de Synthetic Playback para permitir que el agente soporte el proxy en sentido ascendente, a fin de poder supervisar las solicitudes HTTP de las aplicaciones web internas a las aplicaciones web externas.

Procedimiento

- Para configurar y habilitar el soporte de proxy en sentido ascendente para el agente, realice los pasos siguientes.
  a) Como usuario root, configure los valores de proxy ejecutando los mandatos siguientes en la línea de mandatos.

```
cd dir_instalación/agent/lx8266/sn/bin
#./set_proxy.sh
```

  Cuando se le solicite, especifique la vía de acceso de instalación del agente; la vía de acceso predeterminada es `/opt/ibm/apm/agent`. Especifique el número para el tipo de proxy que desee configurar para el Agente de Synthetic Playback.

  Por ejemplo:

```
# cd /dir_instalación/agent/lx8266/sn/bin/
#./set_proxy.sh
especifique la vía de acceso de instalación del agente; el valor predeterminado es
(/opt/ibm/apm/agent)
la vía de acceso de instalación del agente es: /opt/ibm/apm/agent
especifique el número de tipo de proxy:
1 proxy del sistema
2 proxy manual
3 proxy de pac
4 sin proxy
```

  b) Especifique *dir_instalación*`/bin/synthetic_playback-agent.sh start` para reiniciar el agente.
- Linux Para inhabilitar el soporte de proxy en sentido ascendente para el agente, ejecute de nuevo el mandato `./set_proxy.sh` y seleccione `4 sin proxy`. A continuación, reinicie el agente.

Configuración de la supervisión de Tomcat

Puede configurar el Monitoring Agent for Tomcat con los valores predeterminados o personalizados para supervisar los recursos de servidores de aplicaciones Tomcat. El agente puede configurarse en sistemas Windows y Linux.

Antes de empezar

Revise los requisitos previos de hardware y software. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de Tomcat.

Acerca de esta tarea

El Agente de Tomcat es un agente de varias instancias; debe crear la primera instancia e iniciar el agente de forma manual. El nombre de sistema gestionado incluye el nombre de instancia que especifique, por ejemplo, *nombre_instancia*`:`*nombre_host*`:`*pc*, donde *pc* es el código de producto de dos caracteres. El nombre de sistema gestionado está limitado a 32 caracteres. El nombre de instancia que especifique está limitado a 28 caracteres, excluyendo la longitud del nombre de host. Por ejemplo, si especifica `TOMCAT2` como nombre de instancia, el nombre de sistema gestionado será `TOMCAT2:nombrehost:OT`. Si especifica un nombre de instancia largo, el nombre de sistema gestionado queda truncado y el código de agente no se visualiza completamente.

Para evitar problemas de permisos al configurar el agente, asegúrese de utilizar el mismo ID de usuario root o no root que se utilizó para instalarlo. Si ha instalado el agente mediante un usuario seleccionado y desea configurar el agente mediante un usuario distinto, consulte "Configuración de agentes como usuarios no root" en la página 191. Si ha instalado y configurado el agente mediante un usuario seleccionado y desea iniciar el agente mediante un usuario distinto, consulte "Inicio de agentes mediante un usuario no root" en la página 1047.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Configuración del Agente de Tomcat con los valores predeterminados

Puede utilizar los valores predeterminados del Agente de Tomcat para supervisar el servidor Tomcat. No es necesario proporcionar más información de configuración aparte del nuevo nombre de instancia.

Antes de empezar

Antes de configurar el agente con los valores predeterminados, asegúrese de cumplir los requisitos previos siguientes:

- El agente está instalado en el directorio predeterminado.
- El URL de servicio JMX utiliza el puerto 8686.
- El servidor Tomcat está configurado sin la autorización de JMX.

Acerca de esta tarea

Recuerde: Cuando configura el agente con los valores predeterminados, la recopilación de datos de rastreo de transacciones y diagnóstico detallado no está habilitada.

Procedimiento

1. Ejecute el mandato siguiente:
   Linux `dir_instalación/bin/tomcat-agent.sh config nombre_instancia dir_instalación/samples/tomcat_silent_config.txt`
   Windows `dir_instalación\bin\tomcat-agent.bat config nombre_instancia dir_instalación\samples\tomcat_silent_config.txt`
   Donde
   dir_instalación
   El directorio de instalación del Agente de Tomcat.
   nombre_instancia
   El nombre que desea dar a la instancia.
2. Ejecute el mandato siguiente para iniciar el agente:
   Linux `dir_instalación/bin/tomcat-agent.sh start nombre_instancia`
   Windows `dir_instalación\bin\tomcat-agent.bat start nombre_instancia`

Qué hacer a continuación

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del agente en sistemas Windows

Puede configurar el agente en sistemas operativos Windows mediante la ventana **IBM Performance Management**.

Antes de empezar
Asegúrese de que se cumplen los requisitos previos siguientes:

- Java está instalado en el servidor Tomcat donde está instalado el agente.
- La versión de JDK 1.6 o posterior se ha establecido en la solicitud desde la que se instala el instalador del agente.
- JMX remoto está habilitado para el servidor Tomcat. Para obtener más información, consulte Habilitación de JMX remoto.
- El servidor Tomcat se está ejecutando.

Acerca de esta tarea
Puede configurar el agente desde el indicador de mandatos. Para conocer los detalles, siga los pasos indicados en el tema "Configuración del Agente de Tomcat en sistemas Linux" en la página 834 y ejecute los mandatos con la extensión .bat en lugar de la extensión .sh. El procedimiento siguiente explica la configuración del agente mediante el panel de configuración del agente.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en **Monitoring Agent for Tomcat**.
3. Pulse **Configurar agente**.

   Atención: si **Configurar agente** no está disponible, pulse **Reconfigurar**.
4. En la ventana **Nombre de instancia**, especifique un nombre exclusivo para la instancia del Agente de Tomcat y pulse **Aceptar**.

   Restricción: MSN no debe superar los 32 caracteres.
5. En el campo **SERVER NAME**, especifique un nombre exclusivo para identificar el servidor Tomcat que se está supervisando.
6. En la ventana **Valores de parámetro Java**, realice una de las acciones siguientes:
   - Pulse **Siguiente** para aceptar la ubicación predeterminada donde está instalado Java. La vía de acceso de instalación predeterminada es `C:\IBM\APM\java\java80_x64\jre`.
   - En el campo **Directorio inicial de Java**, especifique la vía de acceso si IBM Java se ha instalado en una vía de acceso diferente.
7. En la ventana **Servidor compatible con JSR-160**, especifique los detalles de los parámetros siguientes:
   a) En el campo **ID de usuario de JMX**, especifique el ID del usuario que se utiliza para conectarse al servidor Tomcat MBean cuando la autorización JMX está habilitada en Tomcat.
   b) En el campo **Contraseña de JMX**, especifique la contraseña del usuario de JMX que se utiliza para conectarse al servidor Tomcat MBean cuando la autorización JMX está habilitada en Tomcat.
   c) En el campo **URL de servicio de JMX**, especifique el URL que se utiliza para conectarse al servidor Tomcat MBean.

      El formato del URL es `service:jmx:rmi:///jndi/rmi://`*`nombre_host`*`:`*`número_puerto`*`/jmxrmi`. El URL predeterminado es válido si el servidor se ejecuta en el host local y utiliza el puerto 8686 como puerto JMX. Puede modificar el nombre de host y el número de puerto del URL, conservando el mismo formato.
   d) En la lista **Configuración del recopilador de datos**, seleccione Sí si desea habilitar la recopilación de datos de rastreo de transacciones y de análisis detallado.
8. En la ventana **Monitoring Agent for Tomcat**, pulse la instancia del Agente de Tomcat con el botón derecho del ratón y pulse **Iniciar**.
9. Habilite la recopilación de datos de Rastreo de transacciones y Búsqueda en profundidad y reinicie el servidor Tomcat.

Qué hacer a continuación

Si el Agente de Tomcat se ejecuta como un servicio, después de configurar el agente en Windows, configure el recopilador de datos de Tomcat. Para obtener más información, consulte "Configuración del recopilador de datos de Tomcat " en la página 833.

Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Proporcionar una política de seguridad local para ejecutar Monitoring Agent for Tomcat en Windows con un usuario no administrador

Hay políticas de seguridad local disponibles para que un usuario no administrador ejecute un Monitoring Agent for Tomcat en Windows.

Acerca de esta tarea

Se aplica una combinación de las dos siguientes políticas de seguridad local para que un usuario no administrador ejecute el Agente de Tomcat en Windows. Para el inicio/detención, configuración y verificación de datos de un Agente de Tomcat, se aplican estas dos políticas.

1. Depurar programas.
2. Iniciar sesión como servicio.

Siga el procedimiento indicado para otorgar los permisos de seguridad local para un usuario no administrador.

Procedimiento

1. Vaya a TEMA y cambie el inicio del agente de Tomcat con usuario no administrador.
2. Añada el usuario no administrador bajo la carpeta de instalación del agente de Tomcat y otórguele permisos completos.
3. Añada el usuario no administrador bajo la clave de registro HKEY_LOCAL_MACHINE y pulse **Permisos completos**.
4. Ejecute el mandato **`secpol.msc`** en **startmenu** para abrir las políticas de seguridad locales.
5. A continuación, para añadir el usuario no administrador a las políticas, consulte "Permisos de política de seguridad local" en la página 832.
6. Reinicie el agente de Tomcat.
7. Compruebe el estado de los agentes de Tomcat y verifique los datos en el portal de APM.

Permisos de política de seguridad local

Otorgar el permiso Depurar programas

Acerca de esta tarea

Para otorgar el permiso Depurar programas, siga el procedimiento de Agente de Tomcat como se describe aquí:

Procedimiento

1. Pulse **Inicio > Herramientas administrativas > Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.
2. Expanda **Políticas locales** y pulse **Asignación de derechos de usuario**. Se abre la lista de derechos de usuario.
3. Realice una doble pulsación en la política **Depurar programas**. Se abre la ventana **Propiedades de Depurar programas**.
4. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.

5. En el campo Especificar los nombres de objeto a seleccionar, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
6. Pulse **Aceptar**.

Otorgar el permiso Iniciar sesión como servicio

Acerca de esta tarea
Para otorgar el permiso Iniciar sesión como servicio, siga el procedimiento de Agente de Tomcat como se describe aquí.

Procedimiento

1. Pulse **Inicio > Herramientas administrativas > Política de seguridad local**. Se abrirá la ventana **Configuración de la seguridad local**.
2. Expanda **Políticas locales** y pulse **Asignación de derechos de usuario**. Se abre la lista de derechos de usuario.
3. Realice una doble pulsación en la política **Iniciar sesión como servicio**. Se abre la ventana **Propiedades de Iniciar sesión como servicio**.
4. Pulse **Añadir usuario o grupo**. Se abre la ventana **Seleccionar usuarios o grupos**.
5. En el campo Especificar los nombres de objeto a seleccionar, especifique el nombre de la cuenta de usuario a la que desea asignar los permisos y, a continuación, pulse **Aceptar**.
6. Pulse **Aceptar**.

Configuración del recopilador de datos de Tomcat
Si el Agente de Tomcat se ejecuta como un servicio, después de configurar el agente en Windows, configure el recopilador de datos de Tomcat siguiendo las instrucciones indicadas a continuación.

Acerca de esta tarea

Después de configurar e iniciar la instancia de Agente de Tomcat, ésta genera o actualiza el archivo `setenv.bat` de `/INICIO_CANDLE/setenv_<nombre_instancia>.bat`. Este archivo contiene los parámetros de configuración necesarios para la configuración del recopilador de datos de Tomcat.

Procedimiento

1. Abra la ventana **Propiedades de Apache Tomcat** y pulse **Java**.
2. Abra `setenv_<nombreInstancia>.bat` desde la ubicación `/INICIO_CANDLE/setenv_<nombre_instancia>.bat`
3. Copie el valor del parámetro **JAVA_OPTS** de `setenv_<nombre_instancia>.bat` que se muestra en el bloque:

```
agentlib:am_ibm_16=C:\IBM\APM\otdchome\7.3.0.13.0\runtime\TOMTKWIN1
-Xbootclasspath/p:C:\IBM\APM\otdchome\7.3.0.13.0\toolkit\lib\bcm-bootstrap.jar
-Djava.security.policy=C:\IBM\APM\otdchome\7.3.0.13.0\itcamdc\etc\datacollector.policy
-Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=
C:\IBM\APM\otdchome\7.3.0.13.0\runtime\TOMTKWIN1\TOM_TK_1_DCManual.txt
-Dcom.ibm.tivoli.itcam.serverHome=C:\TOMCAT_9\apache-tomcat-9.0.5\apache-tomcat-9.0.5
-Dam.home=C:\IBM\APM\otdchome\7.3.0.13.0\itcamdc
-Dcom.ibm.tivoli.itcam.toolkit.runtime.dir=C:\IBM\APM\otdchome\7.3.0.13.0\runtime
```

4. Pegue este valor en el recuadro de texto **Opciones de Java** de la pestaña **Java** de **Propiedades de Apache Tomcat**.
5. Pulse **Aplicar**.
6. Vaya a **Panel de control** y pulse **Sistema** > **Configuración avanzada** > **Variables de entorno...**.
7. En **Variables del sistema**, edite la variable *PATH* añadiendo la vía de acceso de archivo `<inicio_OTDC>\toolkit\lib\win64;<INICIO_OTDC>/toolkit\lib\win64\ttapi` y pulse **Aceptar**

Nota: Sustituya <inicio_OTDC> por la vía de acceso real del directorio de instalación del kit de herramientas. Por ejemplo, `C:\IBM\APM\otdchome\7.3.0.13.0\toolkit\lib\win64;C:\IBM\APM\otdchome\7.3.0.13.0\toolkit\lib\win64\ttapi`

8. Pulse **NUEVA** para añadir una variable *RUNTIME_DIR*.
9. Añada **Nombre de variable** como *RUNTIME_DIR* y **Vía de acceso de variable** como `C:\IBM\APM\otdchome\7.3.0.13.0\runtime`. Esta vía de acceso está disponible en `setenv_<nombe_instancia>.bat`
10. Reinicie Windows. Asegúrese de que el inicio del servicio de Tomcat esté establecido en Automático.

Configuración del Agente de Tomcat en sistemas Linux

Ejecute el script de configuración y responda a las solicitudes para configurar el Agente de Tomcat en sistemas Linux.

Antes de empezar

- JMX remoto está habilitado para el servidor Tomcat. Para obtener más información, consulte Enabling JMX Remote.
- El servidor Tomcat se está ejecutando.

Procedimiento

1. Ejecute el mandato siguiente:
   dir_instalación`/bin/tomcat-agent.sh config` *nombre_instancia*
   Donde *nombre_instancia* es el nombre que desea dar a la instancia.
2. Cuando se le solicita que especifique un valor para SERVER, especifique un nombre exclusivo para identificar el servidor Tomcat que se está supervisando y pulse Intro.
3. Cuando se le solicite que especifique un valor para el `directorio inicial de Java`, pulse Intro para aceptar la ubicación predeterminada donde está instalada la máquina virtual Java. La ubicación predeterminada es `/opt/ibm/apm/agent/JRE/lx8266/jre`. Si el agente no está instalado en el directorio predeterminado, especifique *dir_instalación*`/JRE/lx8266/jre`.
4. Cuando se le solicite que especifique un valor para `ID de usuario de JMX`, especifique el ID del usuario que se conecta al servidor Tomcat MBean. Si la autorización de JMX no está habilitada, pulse la tecla Intro.
5. Cuando se le solicite que especifique un valor para la `contraseña de JMX`, especifique la contraseña del usuario de JMX y confírmela. Si no está habilitada la autorización de JMX, pulse la tecla Intro.
6. Cuando se le solicite que especifique un valor para `URL de servicio de JMX`, pulse la tecla Intro para aceptar el URL predeterminado o especifique otro URL de servicio para conectarse al servidor Tomcat MBean.
   El formato del URL es `service:jmx:rmi:///jndi/rmi://`*nombre_host*`:`*número_puerto*`/jmxrmi`. El URL predeterminado es válido si el servidor se ejecuta en el host local y utiliza el puerto 8686 como puerto JMX. Puede modificar el nombre de host y el puerto del URL, conservando el mismo formato.
7. Cuando se le solicite que especifique un valor para la `Configuración del recopilador de datos`, especifique 1 y pulse Intro para habilitar la recopilación de datos de rastreo de transacciones y análisis detallado.
8. Ejecute el mandato siguiente para iniciar el agente:
   dir_instalación`/bin/tomcat-agent.sh start` *nombre_instancia*
9. Habilite la recopilación de datos de Rastreo de transacciones y Búsqueda en profundidad y reinicie el servidor Tomcat.

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Configuración del Agente de Tomcat mediante el archivo de respuestas silencioso

Puede utilizar el archivo de respuestas silencioso para configurar el Agente de Tomcat sin responder a solicitudes.

Procedimiento

1. En un editor de texto, abra el archivo `tomcat_silent_config.txt` que está disponible en la siguiente vía de acceso:
   dir_instalación`/samples`
2. Para el parámetro **KOT_SERVER**, especifique un nombre exclusivo para identificar el servidor Tomcat que se está supervisando.
3. En el parámetro **Java home**, especifique la vía de acceso donde está instalada la máquina virtual Java. La ubicación predeterminada es `/opt/ibm/apm/agent/JRE/lx8266/jre`. Si el agente no está instalado en el directorio predeterminado, especifique *dir_instalación*`/JRE/lx8266/jre`.
4. En el parámetro **ID de usuario de JMX**, especifique el ID del usuario que utiliza para conectarse al servidor Tomcat MBean. Debe especificar un valor para este parámetro si está habilitada la autorización JMX en Tomcat.
5. En el parámetro **Contraseña de JMX**, especifique la contraseña del usuario de JMX. Debe especificar un valor para este parámetro si está habilitada la autorización JMX en Tomcat.
6. En el parámetro **URL de servicio de JMX**, especifique el URL de servicio para conectarse al servidor Tomcat MBean. El formato del URL es `service:jmx:rmi:///jndi/rmi://`*nombre_host*`:`*número_puerto*`/jmxrmi`. El URL predeterminado es válido si el servidor se ejecuta en el host local y utiliza el puerto 8686 como puerto JMX. Puede modificar el nombre de host y el número de puerto del URL, conservando el mismo formato.
7. Para el parámetro **KOT_DCCONFIGURATION**, especifique `Sí` si desea habilitar la recopilación de datos de rastreo de transacciones y análisis detallado.
8. Guarde y cierre el archivo `tomcat_silent_config.txt` y ejecute el mandato siguiente para actualizar los valores de configuración del agente:
   Linux *dir_instalación*`/bin/tomcat-agent.sh config` *nombre_instancia* *dir_instalación*`/samples/tomcat_silent_config.txt`
   Windows *dir_instalación*`/bin/tomcat-agent.bat config` *nombre_instancia* *dir_instalación*`/samples/tomcat_silent_config.txt`
   Donde *nombre_instancia* es el nombre que desea dar a la instancia y *dir_instalación* es el directorio de instalación del Agente de Tomcat.
9. Ejecute el mandato siguiente para iniciar el agente:
   Linux *dir_instalación*`/bin/tomcat-agent.sh start` *nombre_instancia*
   Windows *dir_instalación*`/bin/tomcat-agent.bat start` *nombre_instancia*
10. Si habilita la recopilación de datos de rastreo de transacciones y búsqueda en profundidad, reinicie el servidor Tomcat.

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Habilitación de la recopilación de datos de diagnóstico y rastreo de transacciones

En la página **Configuración de agente**, puede habilitar o inhabilitar la recopilación de datos de rastreo de transacciones o diagnóstico.

Acerca de esta tarea
Si habilita la recopilación de datos de rastreo de transacciones, el agente recopila datos de los componentes siguientes:

- Servlet JSP
- Aplicaciones EJB
- JMS

Procedimiento

Complete los pasos siguientes para configurar la recopilación de datos para cada sistema gestionado.

1. Inicie la sesión en la Consola de Cloud APM.
2. En la barra de navegación, pulse **Configuración del sistema** > **Configuración del agente**.
   Se mostrará la página **Configuración del agente**.
3. Pulse la pestaña **Tomcat**.
4. Marque los recuadros de selección de los sistemas gestionados para los que desea configurar la recopilación de datos y lleve a cabo una de las acciones siguientes de la lista **Acciones**.
   - Para habilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Habilitado**. El estado de la columna **Rastreo de transacciones** se actualiza a Habilitado para cada sistema gestionado seleccionado.
   - Para habilitar la recopilación de datos de diagnóstico, seleccione **Establecer modalidad de diagnóstico** > **Sólo Modalidad de diagnóstico habilitada**. El estado de la columna Modalidad de diagnóstico se actualiza a Habilitado para cada sistema gestionado seleccionado.
   - Para habilitar la recopilación de datos de diagnóstico y el rastreo de método, seleccione **Establecer modalidad de diagnóstico** > **Modalidad de diagnóstico y rastreo de método habilitados**. El estado de las columnas Modalidad de diagnóstico y Rastreo de método se actualiza a Habilitado para cada sistema gestionado seleccionado.
   - Para inhabilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Inhabilitado**. El estado de la columna **Rastreo de transacciones** se actualiza a Inhabilitado para cada sistema gestionado seleccionado.
   - Para inhabilitar la recopilación de datos de diagnóstico, pulse **Establecer la modalidad de diagnóstico** > **Modalidad de diagnóstico y rastreo de método inhabilitados**. El estado de las columnas **Modalidad de diagnóstico y Rastreo de método** se actualiza a Inhabilitado para cada sistema gestionado seleccionado.

Qué hacer a continuación
Inicie sesión en la Consola de Cloud APM para ver los datos de diagnóstico y rastreo de transacciones recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Actualizar o cambiar el servidor de aplicaciones Tomcat

Para actualizar o cambiar el servidor de aplicaciones Tomcat después de la configuración de Agente de Tomcat, siga los pasos que se proporcionan en este tema. Estos pasos son comunes para ambos, Tomcat configurado a través de Windows y Linux.

Procedimiento

1. Detenga la instancia de Agente de Tomcat y el servidor Tomcat.
2. Vaya a <TOMCAT_SERVER>/bin y abra el archivo setenv.sh en un editor.
3. Elimine todos los parámetros de inicio para el recopilador de datos de setenv.sh. Elimine las siguientes líneas del archivo

```
export LD_LIBRARY_PATH="<CANDLE_HOME>/otdchome/7.3.0.13.0/toolkit/lib/lx8266"
export RUNTIME_DIR="<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime"
```

```
export JAVA_OPTS="-agentlib:am_ibm_16=<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime/
<Tomcat_Application_
Server> -
Xbootclasspath/p:<CANDLE_HOME>/otdchome/7.3.0.13.0/toolkit/lib/bcm-bootstrap.jar -
Djava.security.policy=<CANDLE_HOME>/otdchome/7.3.0.13.0/itcamdc/etc/datacollector.policy -
Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime/
<Tomcat_
Application_Server>/<Agent_Instance>_DCManual.txt -
Dcom.ibm.tivoli.itcam.serverHome=<TOMCAT_HOME> -
Dam.home=<CANDLE_HOME>/otdchome/7.3.0.13.0/itcamdc -
Dcom.ibm.tivoli.itcam.toolkit.runtime.dir=<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime"
```

4. Guarde los cambios e inicie el servidor Tomcat
5. Vuelva a configurar Agente de Tomcat para actualizar o cambiar el servidor de aplicaciones Tomcat
6. Actualice o cambie solo el servidor de aplicaciones Tomcat y no cambie ningún otro valor configuración
7. Inicie la instancia de Agente de Tomcat
8. Compruebe que el archivo `setenv.sh` se ha actualizado con el nuevo servidor de aplicaciones Tomcat en los parámetros de inicio para el recopilador de datos
9. Reinicie el servidor Tomcat
10. Verifique que los cambios realizados en el servidor de aplicaciones Tomcat se reflejan en la máquina del agente y en el panel de instrumentos de IBM Cloud Application Performance Management
    - Verifique el cambio del servidor de aplicaciones Tomcat en Ubicación de `<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime/<Servidor_Aplicaciones_Tomcat>` en la máquina de agente
    - Verifique el cambio del servidor de aplicaciones Tomcat en la página **Topología de transacciones agregada** y el atributo *appserver* bajo el grupo de atributos *KOT_Server* en el panel de instrumentos de IBM Cloud Application Performance Management

Configuración de la supervisión de VMware VI

Después de instalar el Monitoring Agent for VMware VI, debe crear la primera instancia e iniciar manualmente el agente para que éste pueda recopilar datos de la VMware Virtual Infrastructure que se está supervisando.

Antes de empezar

- Revise los requisitos previos de hardware y software.
- Cree un ID de usuario en VMware Virtual Infrastructure. El agente utiliza este ID de usuario para conectarse al vCenter de VMware para supervisar VMware Virtual Infrastructure. Asegúrese de tener privilegios "System.View" y "System.Read" sobre todos los vCenters y servidores ESX que se están supervisando. Para obtener información acerca de cómo crear el ID de usuario, consulte la documentación de VMware relativa a la gestión de usuarios, grupos, permisos y roles.
- Determine si el vCenter está configurado para la comunicación SSL. Si se ha configurado, debe configurar el Agente de VMware VI para utilizar SSL para comunicarse con el vCenter.
  - Para determinar si el vCenter utiliza SSL para la comunicación, utilice el URL `https://`*`direcciónIPvCenter`* para acceder al vCenter. Si puede acceder al vCenter, indica que el vCenter utiliza SSL para comunicarse a través de la red.
  - Para configurar el Agente de VMware VI para que utilice SSL para comunicarse con el vCenter, siga los pasos que se describen en "Habilitación de la comunicación SSL con orígenes de datos de VMware VI" en la página 839.
- Decida el número de instancias de agente que necesita para supervisar VMware Virtual Infrastructure. Para obtener información acerca del dimensionamiento de las instancias de agente en función del entorno de supervisión, consulte la sección "Dimensionamiento y planificación del despliegue del Agente de VMware VI" en la página 838.

Acerca de esta tarea

El Agente de VMware VI es un agente de múltiple instancia. A diferencia de un agente de instancia única, que puede configurar para supervisar y recopilar datos sólo para una aplicación supervisada, el Agente de VMware VI puede tener varias instancias configuradas que se conecten a varios servidores de vCenter y supervisen remotamente VMware Virtual Infrastructure.

Los parámetros de configuración definen los orígenes de datos de VMware VI que se supervisan y una conexión a VMware vCenter, vCenter Server Appliance o a un servidor VMware ESX individual. Para conocer las versiones soportadas de estas aplicaciones, consulte Software Product Compatibility Reports for the Agente de VMware VI.

La versión del producto y la versión del agente a menudo difieren. Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Debe configurar manualmente el agente para ver datos de todos los atributos de agente.

- Para configurar el agente en sistemas operativos Windows, puede utilizar la ventana **IBM Performance Management** o el archivo de respuestas silencioso.
- Para configurar el agente en sistemas operativos Linux, puede ejecutar el script y responder a las solicitudes, o utilizar el archivo de respuestas silencioso.

Dimensionamiento y planificación del despliegue del Agente de VMware VI

El número de instancias de agente que puede configurar en un solo sistema depende de la disponibilidad y utilización de recursos del mismo.

La tabla siguiente categoriza el entorno VMware en diversos tamaños con el tamaño de almacenamiento dinámico de Java necesario:

Tabla 218. Tamaño del entorno VMware y del almacenamiento dinámico de Java

Tamaño del entorno VMware	Número de servidores ESX	Tamaño de almacenamiento dinámico de Java
Entorno pequeño	Un servidor vCenter que gestiona hasta 125 servidores ESX(i) y de 300 a 1500 invitados.	**-Xmx2048m** (2 GB)
Entorno mediano	Un servidor vCenter que gestiona entre 125 y 250 servidores ESX(i) y de 1500 a 4000 invitados.	**-Xmx4096m** (4 GB)
Entorno grande	Un servidor vCenter que gestiona entre 250 y 500 servidores ESX(i) y de 4000 a 7500 invitados.	**-Xmx8192m** (8 GB)
Entorno muy grande	Un servidor vCenter que gestiona más de 500 servidores ESX(i) y más de 7500 invitados.	**-Xmx16384m** (16 GB)

Para aumentar el tamaño de almacenamiento dinámico del proveedor de datos de Java, complete los pasos que se describen en "Aumento del tamaño de almacenamiento dinámico de Java" en la página 845.

Para que las instancias de agente supervisen correctamente el entorno, el servidor en el que instale el agente debe tener recursos de memoria adecuados para dar cabida a los datos recopilados por estas instancias de agente. Una única instancia del Agente de VMware VI requiere aproximadamente de 300 a 400 MB para supervisar un entorno pequeño. Consulte las directrices siguientes acerca del número de instancias de agente que deben configurarse:

- Utilice una sola instancia para supervisar un solo vCenter. No utilice la misma instancia para supervisar varios vCenters.
- En un entorno sin clúster, utilice una sola instancia para supervisar un máximo de 8 servidores ESX pequeños (100 a 200 máquinas virtuales en un servidor ESX). No configure varios servidores ESX individuales bajo la instancia de agente única.
- Utilice varias instancias de agente del Agente de VMware VI para supervisar un entorno que contenga varios vCenters. Antes de configurar varias instancias, asegúrese de contar con recursos de memoria adecuados en el sistema en el que instala el agente.

Habilitación de la comunicación SSL con orígenes de datos de VMware VI

Antes de configurar el agente para comunicarse de forma segura con sus orígenes de datos de VMware VI mediante SSL, debe añadir un certificado SSL de origen de datos al almacén de confianza del certificado del agente.

Acerca de esta tarea

Importante: La siguiente información sólo se aplica si el agente se configura para validar certificados SSL.

Si la validación de certificados SSL está desactivada, el Agente de VMware VI se conecta a orígenes de datos de VMware, incluso si sus certificados SSL están caducados, no son de confianza o no son válidos. Sin embargo, al desactivar la validación de certificados SSL, la seguridad podría comprometerse, por lo que esta operación debe hacerse con precaución.

Si un origen de datos de VMware utiliza un certificado SSL que está firmado por una entidad emisora de certificados común (por ejemplo, Verisign, Entrust, o Thawte), no es necesario añadir certificados al almacén de certificados del Agente de VMware VI. Sin embargo, si el origen de datos utiliza un certificado que no esté firmado por una entidad emisora de certificados común, que es lo que sucede de forma predeterminada, debe añadir el certificado al almacén de confianza para permitir que el agente se conecte y recopile datos satisfactoriamente .

Nota:

1. El archivo de certificados de VMware predeterminado se denomina `rui.crt`.
2. Para un centro virtual, el archivo del certificado SSL se encuentra de forma predeterminada en la vía de acceso siguiente:

   `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL`
3. Para un servidor ESX, el archivo del certificado SSL se encuentra de forma predeterminada en el directorio `/etc/vmware/ssl`.

Procedimiento

1. Copie el archivo de certificados del origen de datos al sistema del agente.
2. Coloque el archivo de certificados en un directorio de su elección en el sistema del agente. No sobrescriba los archivos de certificados. Utilice una etiqueta y nombre de archivo exclusivos para cada certificado que añada.
3. Utilice el mandato *keytool* para añadir un certificado de origen de datos al almacén de confianza de certificados del agente:

   ```
   keytool -import -noprompt -trustcacerts -alias AliasCertificado -file
   ArchivoCertificado -keystore AlmacénConfianza -storepass
   ContraseñaAlmacénConfianza
   ```

   Donde

AliasCertificado

Se añade una referencia exclusiva para cada certificado al almacén de confianza del agente. Por ejemplo, un alias adecuado para el certificado de *origendatos.ejemplo.com* sería *origendatos*.

ArchivoCertificado

Vía de acceso completa y el nombre de archivo para el certificado de origen de datos de VMware que se va a añadir al almacén de confianza.

Almacén de confianza

Nombre de archivo y vía de acceso completos a la base de datos de certificados del Agente de VMware VI. Utilice la siguiente vía de acceso y nombre de archivo:

- Windows (64 bits): `dir_instalación\tmaitm6_x64\kvm.truststore`
- Linux (64 bits): `dir_instalación/lx8266/vm/etc/kvm.truststore`

ContraseñaAlmacénConfianza

ITMVMWAREVI es la contraseña predeterminada para el almacén de confianza del Agente de VMware VI. Para cambiar la contraseña, consulte la documentación de Java Runtime a fin de obtener información sobre las herramientas que deben utilizarse.

Importante: Para poder utilizar el mandato *keytool*, debe constar el directorio bin de Java Runtime en la vía de acceso. Utilice los mandatos siguientes:

- Windows (64 bits): `set PATH=%PATH%;dir_instalación\java\java70_x64\jre\bin`
- Linux (64 bits): `PATH="$PATH":/opt/ibm/apm/agent/JRE/lx8266/bin`

4. Después de añadir todos los certificados de origen de datos, inicie el agente de supervisión.

Qué hacer a continuación
Complete la configuración del agente.

Configuración del agente en sistemas Windows

Puede configurar el agente en sistemas operativos Windows mediante la ventana **IBM Performance Management**. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Acerca de esta tarea

El Agente de VMware VI proporciona valores predeterminados para algunos parámetros. Puede especificar diferentes valores para estos parámetros.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**.
2. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón **Monitoring Agent for VMware VI** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar el agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar el agente de nuevo, pulse **Reconfigurar**.
3. En la ventana Monitoring Agent for VMware VI, realice los pasos siguientes:
   a) Escriba un nombre exclusivo para la instancia del Agente de VMware VI y pulse **Aceptar**.
   b) En la pestaña **Proveedor de datos**, especifique valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.
   c) En la pestaña **Origen de datos**, especifique valores para los parámetros de configuración y, a continuación, pulse **Siguiente**.

      El Agente de VMware VI es un agente de múltiples orígenes de datos. Puede supervisar varios orígenes de datos desde el mismo agente.

- Si desea configurar un nuevo origen de datos, pulse **Nuevo**.
- Si desea eliminar un origen de datos existente, pulse **Suprimir**.

Para obtener información sobre los parámetros de configuración de cada pestaña de la ventana Monitoring Agent for VMware VI, consulte los temas siguientes:

- Parámetros de configuración del proveedor de datos
- Parámetros de configuración del origen de datos

4. En la ventana **IBM Performance Management**, pulse con el botón derecho del ratón la instancia que ha configurado y pulse **Iniciar**.

Qué hacer a continuación

- Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

  Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.
- Si está supervisando un entorno VMware grande con más de 500 hosts ESX, es posible que tenga que aumentar el tamaño de almacenamiento dinámico para el proveedor de datos Java. Para obtener más información, consulte "Aumento del tamaño de almacenamiento dinámico de Java" en la página 845.

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

- Para configurar el Agente de VMware VI en modalidad silenciosa, realice los pasos siguientes:
  a) En un editor de texto, abra el archivo `vmware_vi_silent_config.txt` que está disponible en la siguiente vía de acceso:
     – Linux *dir_instalación*`/samples/vmware_vi_silent_config.txt`

       Ejemplo: `/opt/ibm/apm/agent/samples/vmware_vi_silent_config.txt`
     – Windows *dir_instalación*`\samples\vmware_vi_silent_config.txt`

       Ejemplo: `C:\IBM\APM\samples\vmware_vi_silent_config.txt`
  b) En el archivo `vmware_vi_silent_config.txt`, especifique valores para todos los parámetros obligatorios. También puede modificar los valores predeterminados de otros parámetros.

     Para obtener información sobre los parámetros de configuración, consulte los siguientes temas:
     – "Parámetros de configuración del proveedor de datos" en la página 844
     – "Parámetros de configuración del origen de datos" en la página 843
  c) Guarde y cierre el archivo `vmware_vi_silent_config.txt` y ejecute el mandato siguiente:

– Linux *dir_instalación*/bin/vmware_vi-agent.sh config *nombre_instancia* *dir_instalación*/samples/vmware_vi_silent_config.txt

Ejemplo: **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh config nombre_instancia /opt/ibm/apm/agent/samples/vmware_vi_silent_config.txt**

– Windows *dir_instalación*\bin\vmware_vi-agent.bat config *nombre_instancia* *dir_instalación*\samples\vmware_vi_silent_config.txt

Ejemplo: **C:\IBM\APM\bin\ vmware_vi-agent.bat config nombre_instancia C:\IBM\APM\samples\vmware_vi_silent_config.txt**

Donde

nombre_instancia
Nombre que desea dar a la instancia.

dir_instalación
Vía de acceso donde está instalado el agente.

Importante: Asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

d) Ejecute el mandato siguiente para iniciar el agente:

– Linux *dir_instalación*/bin/vmware_vi-agent.sh start *nombre_instancia*

Ejemplo: **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh start nombre_instancia**

– Windows *dir_instalación*\bin\vmware_vi-agent.bat start *nombre_instancia*

Ejemplo: **C:\IBM\APM\bin\vmware_vi-agent.bat start nombre_instancia**

Qué hacer a continuación

- Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

  Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.
- Si está supervisando un entorno VMware grande con más de 500 hosts ESX, es posible que tenga que aumentar el tamaño de almacenamiento dinámico para el proveedor de datos Java™. Para obtener más información, consulte "Aumento del tamaño de almacenamiento dinámico de Java" en la página 845.

Configuración del agente respondiendo a solicitudes

Para configurar el agente en sistemas operativos Linux, debe ejecutar el script y responder a las solicitudes.

Procedimiento

- Para configurar el agente mediante la ejecución del script y las respuestas a las solicitudes, siga estos pasos:

  a) En la línea de mandatos, ejecute el mandato siguiente:

  dir_instalación/bin/vmware_vi-agent.sh config *nombre_instancia*

  Ejemplo **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh config nombre_instancia**

  Donde

  nombre_instancia
  Nombre que desea dar a la instancia.

  dir_instalación
  Vía de acceso donde está instalado el agente.

b) Responda a las solicitudes haciendo referencia a los temas siguientes:

- "Parámetros de configuración del proveedor de datos" en la página 844
- "Parámetros de configuración del origen de datos" en la página 843

c) Ejecute el mandato siguiente para iniciar el agente:

dir_instalación/bin/vmware_vi-agent.sh start *nombre_instancia*

Ejemplo: **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh start nombre_instancia**

Qué hacer a continuación

- Inicie sesión en la Consola de Cloud APM para ver los datos recopilados por el agente en los paneles de instrumentos. Para obtener información sobre cómo utilizar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

  Si necesita ayuda con la resolución de problemas, consulte el Foro de IBM Cloud APM en developerWorks.
- Si está supervisando un entorno VMware grande con más de 500 hosts ESX, es posible que tenga que aumentar el tamaño de almacenamiento dinámico para el proveedor de datos Java™. Para obtener más información, consulte "Aumento del tamaño de almacenamiento dinámico de Java" en la página 845.

Parámetros de configuración del origen de datos

Al configurar el Agente de VMware VI, puede cambiar los valores predeterminados de los parámetros del origen de datos, como la dirección, el ID de usuario y la contraseña del origen de datos.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del origen de datos.

Tabla 219. Nombres y descripciones de los parámetros de configuración del origen de datos

Nombre de parámetro	Descripción	Campo obligatorio
ID de origen de datos	El ID del origen de datos.	Sí
Dirección de origen de datos	Dirección del origen de datos. Si no desea que el agente valide los certificados SSL, establezca el valor en el nombre de host o la dirección IP del centro virtual VMware o servidor ESX que se está supervisando. Si desea que el agente valide los certificados SSL al utilizar SSL para comunicarse a través de la red, configure el agente mediante el Nombre alternativo de asunto proporcionado por el certificado. Para ver el nombre alternativo de asunto del centro de datos, siga estos pasos: 1. Abra el certificado. 2. En la ventana **Certificado**, pulse la pestaña **Detalles**. 3. Seleccione **Nombre alternativo de asunto** y utilice el valor del Nombre DNS. Por ejemplo, si el valor del Nombre DNS es "ibmesx3v3vc.ITMfVS.com", utilice el valor "ibmesx3v3vc.ITMfVS.com" para el nombre de host.	Sí

Tabla 219. Nombres y descripciones de los parámetros de configuración del origen de datos (continuación)		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Utilizar la conexión SSL al origen de datos	Indica si el agente utiliza una conexión SSL para conectarse a los orígenes de datos de la infraestructura virtual de VMware. Especifique `Sí` si el agente utiliza una conexión SSL para conectarse a los orígenes de datos. De lo contrario, especifique `No`. El valor predeterminado es `Sí`.	Sí
ID de usuario del origen de datos	El ID de usuario que tiene privilegios suficientes para recopilar datos de supervisión, y el origen de datos lo conoce.	Sí
Contraseña del origen de datos	La contraseña del ID de usuario que se ha configurado para acceder al origen de datos.	Sí
Confirmar contraseña de origen de datos	La misma contraseña que ha especificado en el campo **Contraseña de origen de datos**.	

Parámetros de configuración del proveedor de datos

Al configurar el Agente de VMware VI, puede cambiar los valores predeterminados de los parámetros del proveedor de datos, por ejemplo el número máximo de archivos de registro del proveedor de datos, el tamaño máximo del archivo de registro y el nivel de detalle que se incluye en el archivo de registro.

La tabla siguiente contiene descripciones detalladas de los parámetros de configuración del proveedor de datos.

Tabla 220. Nombres y descripciones de los parámetros de configuración del proveedor de datos		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Nombre de instancia	El nombre de la instancia. **Restricción:** el campo **Nombre de instancia** muestra el nombre de la instancia que especifica al configurar el agente por primera vez. Al volver a configurar el agente, no puede cambiar el nombre de instancia del agente.	Sí
Certificados SSL válidos	Indica si el agente valida certificados SSL cuando el agente utiliza SSL para comunicarse por la red. Establezca el valor en `Yes` si desea que el agente valide certificados SSL cuando el agente utilice SSL para comunicarse a través de la red. Establezca el valor en `No` para impedir que el agente valide certificados SSL. El valor predeterminado es `Sí`. Para obtener información acerca de la adición de un certificado de SSL de origen de datos al almacén de confianza de certificado del agente, consulte la sección “Habilitación de la comunicación SSL con orígenes de datos de VMware VI” en la página 839.	Sí
Número máximo de archivos de registro del proveedor de datos	El número máximo de archivos de registro que el proveedor de datos crea antes de grabar encima de los archivos de registro anteriores. El valor predeterminado es 10.	Sí
Tamaño máximo en KB de cada archivo de registro del proveedor de datos	El tamaño máximo en KB que debe alcanzar un archivo de registro del proveedor de datos antes de que el proveedor de datos cree un archivo de registro nuevo. El valor predeterminado es 5190 KB.	Sí

Tabla 220. Nombres y descripciones de los parámetros de configuración del proveedor de datos (continuación)		
Nombre de parámetro	**Descripción**	**Campo obligatorio**
Nivel de detalle en el archivo de registro del proveedor de datos	El nivel de detalle que puede incluirse en el archivo de registro que crea el proveedor de datos. El valor predeterminado es INFO. Los valores válidos son OFF, SEVERE, WARNING, INFO, FINE, FINER, FINEST y ALL.	Sí
KEY_STORE_PASSWORD	**KEY_STORE_PASSWORD** permite al usuario configurar el agente con la nueva contraseña de almacén de claves para el JRE del agente. Tenga en cuenta que este almacén de claves Java no tiene ninguna relación con el almacén de claves de vCenter. No es obligatorio especificar la contraseña en cada configuración. Si este campo se deja en blanco, el agente presupone que se debe utilizar la contraseña de almacén de claves Java predeterminada al utilizar el JRE del agente.	No

Aumento del tamaño de almacenamiento dinámico de Java

Después de configurar el Agente de VMware VI, si está supervisando un gran entorno de VMware Virtual Infrastructure, es posible que tenga que aumentar el tamaño de almacenamiento dinámico para el proveedor de datos de Java.

Acerca de esta tarea

El tamaño máximo de almacenamiento dinámico predeterminado para el proveedor de datos Java es de 256 megabytes. Debe establecer el tamaño máximo de almacenamiento dinámico en un valor adecuado que depende del tamaño del entorno de VMware. Para obtener información sobre los tamaños de almacenamiento dinámico que son necesarios para los diversos entornos de VMware, consulte Tabla 218 en la página 838.

Importante: el sistema en el que instale y configure el Agente de VMware VI debe tener el espacio de memoria adecuado para dar cabida al tamaño de almacenamiento dinámico necesario.

Si surge alguno de los problemas siguientes, es posible que tenga que aumentar el tamaño de almacenamiento dinámico:

- El proveedor de datos de Java se detiene debido a un problema de `javacore` y crea un archivo denominado `javacore.`*`fecha.hora.número`*`.txt` en el directorio `CANDLEHOME\tmaitm6_x64`.
- El archivo `javacore.`*`fecha.hora.número`*`.txt` contiene la serie `java/lang/OutOfMemoryError`.

Procedimiento

- Windows
  Complete los pasos siguientes para establecer un valor de 1 GB como el tamaño de almacenamiento dinámico:
  1. Abra el archivo `%CANDLE_HOME%\TMAITM6_x64\kvm_data_provider.bat`.
  2. Añada la siguiente línea antes de la línea que empieza por `KVM_JVM_ARGS="%KVM_CUSTOM_JVM_ARGS...`:
     ```
     SET KVM_CUSTOM_JVM_ARGS=-Xmx1024m
     ```
  3. Reinicie el agente.
- Linux
  Complete los pasos siguientes para establecer un valor de 1 GB como tamaño de almacenamiento dinámico:

1. Abra el archivo `$CANDLEHOME/lx8266/vm/bin/kvm_data_provider.sh`.
2. Añada la siguiente línea antes de la línea que empieza por `KVM_JVM_ARGS="$KVM_CUSTOM_JVM_ARGS...`:

```
KVM_CUSTOM_JVM_ARGS=-Xmx1024m
```

3. Reinicie el agente.

Configuración de la supervisión de WebLogic

Monitoring Agent for WebLogic proporciona un punto central de supervisión del estado, disponibilidad y rendimiento del entorno de servidor WebLogic. El agente muestra un conjunto completo de métricas para ayudarle a tomar decisiones informadas sobre los recursos de WebLogic, incluyendo máquinas virtuales Java (JVM), Java Message Service (JMS) y Java Database Connectivity (JDBC).

Antes de empezar

- Las instrucciones siguientes son para el release más reciente del agente, a excepción de lo indicado.
- Asegúrese de que los requisitos del sistema del Agente de WebLogic se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Software Product Compatibility Reports (SPCR) para el Agente de WebLogic.
- Antes de configurar el Agente de WebLogic, debe configurarse el servidor Oracle WebLogic completando las tareas siguientes:

  Nota: La mayor parte de la configuración del servidor Oracle WebLogic se realiza utilizando la consola de administración, normalmente en `http://`*`servidor-weblogic`*`:7001/console`.

  1. Configure un usuario supervisor en el grupo Supervisores.
     a. Seleccione el dominio que desea supervisar/editar.
     b. Seleccione **Dominios de seguridad**.
     c. Seleccione el dominio de seguridad (o cree uno si no existe ninguno).
     d. Cree un usuario que se utilizará para comunicarse con WebLogic mediante JMX.
     e. Añada este usuario el grupo Supervisores.
     f. Guarde los cambios en el dominio.
  2. Habilite los puertos de escucha.
     a. Seleccione el dominio que desea supervisar/editar.
     b. En cada servidor que desee supervisar, pulse **Entorno** > **Servidores** > ***Seleccionar un servidor***.
     c. Asegúrese de que el **Puerto de escucha** está habilitado y anote su número de puerto.
     d. Si desea habilitar SSL, asegúrese de que el **Puerto de escucha SSL** está habilitado y establezca también un puerto para SSL.
  3. Habilite las conexiones de servidor JMX MBean.
     a. Seleccione el dominio que desea supervisar/editar.
     b. Seleccione **Configurar** > **Avanzado**.
     c. Seleccione **Servidor Mbean plataforma habilitado**.
     d. Guarde el cambio.
  4. Habilite la opción de protocolo IIOP.
     a. Seleccione el dominio que desea supervisar/editar.
     b. En cada servidor que desee supervisar, pulse **Entorno** > **Servidores** y seleccione un servidor.
     c. Seleccione la **pestaña Protocolo** > ***Seleccionar IIOP***.

d. En la sección **Avanzado**, especifique el nombre de usuario y la contraseña IIOP predeterminados.

e. Guarde el cambio.

5. Habilite SSL.

a. Habilitar tunelado HTTP.

1) Vaya a **Entorno** > **Servidores** > ***Seleccione un servidor*** > **Protocolo** > **General**.

2) Seleccione **Habilitar tunelado HTTP**.

b. Habilite el puerto de escucha SSL.

1) Vaya a **Entorno** > **Servidores** > ***Seleccionar un servidor*** > **Configuración** > **General**.

2) Configure un número de puerto.

Acerca de esta tarea

El Agente de WebLogic es un agente de varias instancias y también un agente de varios subnodos. Puede crear una instancia de agente con varios subnodos, uno para cada servidor WebLogic o puede crear una instancia de agente para cada servidor WebLogic con un subnodo para ese servidor. También puede crear una combinación de cada tipo de configuración. Después de configurar instancias de agente, debe iniciar manualmente cada instancia de agente.

Procedimiento

1. Para configurar el agente en sistemas Windows, utilice la ventana **IBM Performance Management** o el archivo de respuestas silencioso con el archivo de proceso por lotes de configuración de agente.
   - "Configuración del agente en sistemas Windows" en la página 848.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 852.
2. Para configurar el agente en sistemas Linux y UNIX, ejecute el script de configuración del agente y responda a las solicitudes o utilice el archivo de respuestas silencioso,
   - "Configuración del agente respondiendo a solicitudes" en la página 851.
   - "Configuración del agente mediante el archivo de respuestas silencioso" en la página 852.
3. Opcional: Para configurar el rastreo de transacciones, configure instancias de agente individuales para proporcionar datos de rastreo de transacciones y configure el Panel de instrumentos del rendimiento de aplicaciones para visualizar datos de rastreo de transacciones.

   a) Siga el procedimiento de "Configuración del rastreo de transacciones para el Agente de WebLogic" en la página 855.

   b) Siga el procedimiento de "Configuración del Panel de instrumentos del rendimiento de aplicaciones para visualizar datos de rastreo de transacciones para el Agente de WebLogic" en la página 861.

   Nota: La prestación de rastreo de transacciones está disponible para el Agente de WebLogic en la oferta Cloud APM, Advanced. Para el Agente de WebLogic con prestación de supervisión de recursos básica, que se encuentra en la oferta Cloud APM, Base, omita este paso.

Qué hacer a continuación

En la Consola de Cloud APM, vaya al Panel de instrumentos del rendimiento de aplicaciones para ver los datos que se han recopilado. Para obtener más información sobre la utilización de la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

Si no puede ver los datos en los paneles de instrumentos del agente, consulte primero los registros de conexión del servidor y, a continuación, los registros del proveedor de datos. Las vías de acceso predeterminadas a estos registros son los siguientes:

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Si desea recibir ayuda con la resolución de problemas, consulte el Foro de Cloud Application Performance Management.

Configuración del agente en sistemas Windows

Puede configurar el Agente de WebLogic en sistemas operativos Windows utilizando la ventana de IBM Cloud Application Performance Management. Después de actualizar los valores de configuración, debe iniciar el agente para guardar los valores actualizados.

Procedimiento

1. Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. En la ventana **IBM Performance Management**, pulse el botón derecho del ratón en la plantilla **Monitoring Agent for WebLogic** y luego pulse **Configurar agente**.

   Recuerde: Después de configurar una instancia de agente por primera vez, la opción **Configurar el agente** está inhabilitada. Para configurar la instancia de agente de nuevo, púlsela con el botón derecho del ratón y luego pulse **Reconfigurar**.
3. Especifique un nombre de instancia exclusivo y luego pulse **Aceptar**. Utilice solamente letras, números, el carácter de subrayado y el carácter menos en el nombre de la instancia. Por ejemplo: `weblogic01`.

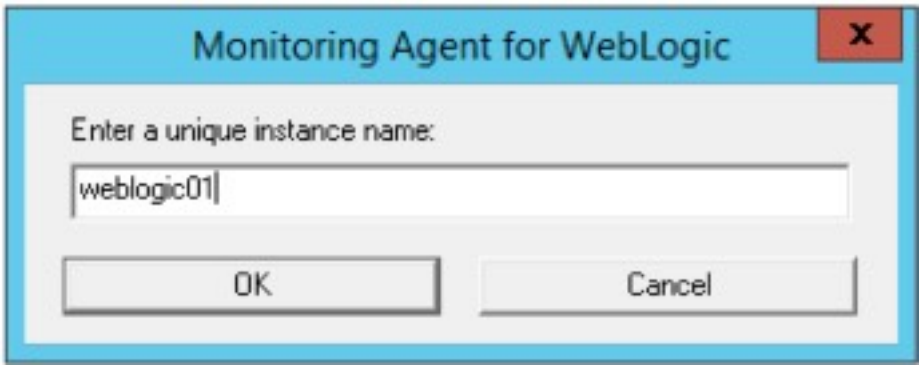


Figura 27. La ventana para especificar un nombre de instancia exclusivo

4. Pulse en **Siguiente** en panel de configuración de agente **Nombre de instancia**.

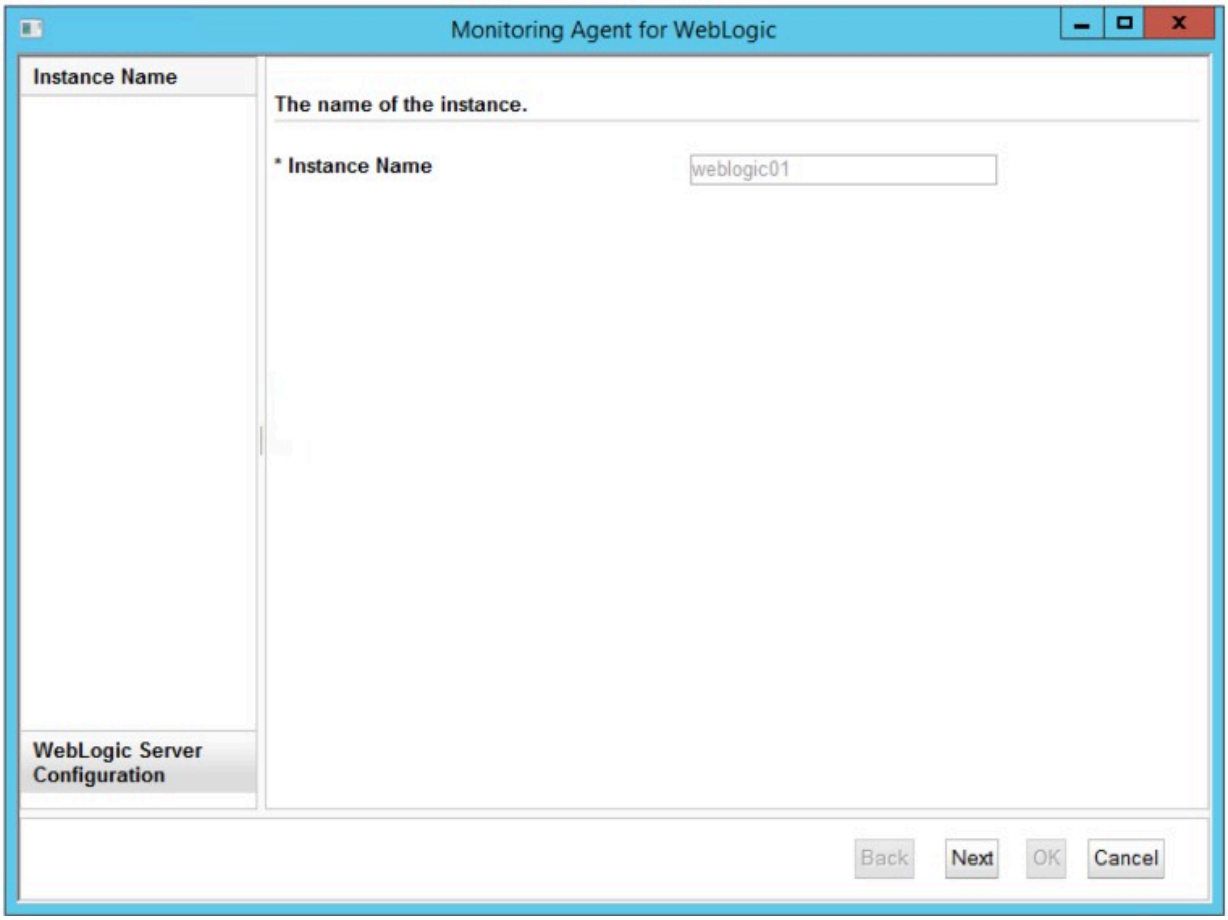


Figura 28. La ventana que muestra el nombre de instancia de agente

5. Especifique los valores de la plantilla de instancia de **Configuración del servidor de WebLogic**.

   Nota: esta sección no corresponde a la configuración de instancia de conexión de servidor de WebLogic. Es una sección de la plantilla destinada a establecer lo que se utiliza como valores predeterminados al añadir las configuraciones de instancia de conexión de servidor de WebLogic reales a partir del paso 6.

   Consulte la sección Tabla 221 en la página 854 para obtener una descripción de cada uno de los parámetros de configuración.

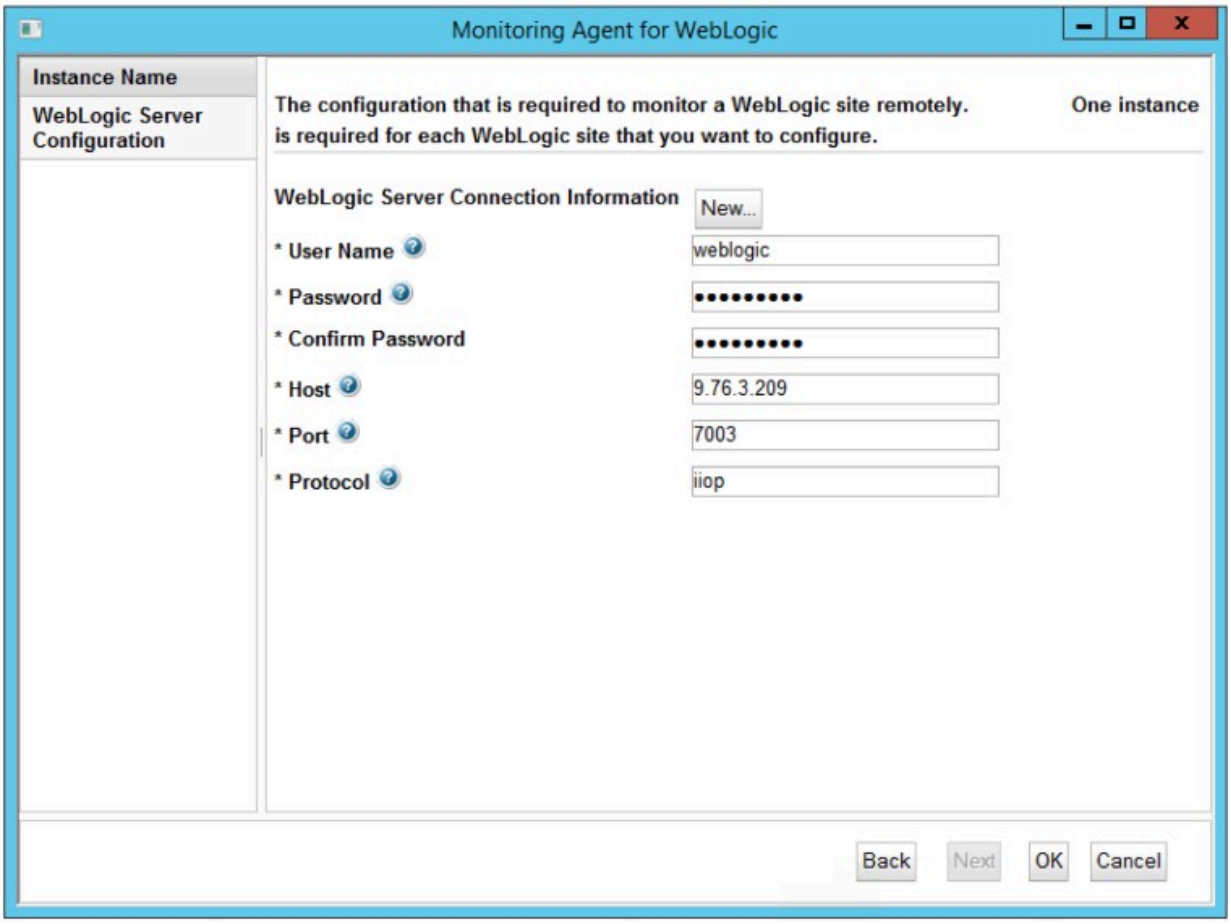


Figura 29. La ventana para especificar valores de plantilla de instancia de conexión de servidor de WebLogic

6. Pulse **Nuevo**, especifique valores de instancia de conexión del servidor de WebLogic y, a continuación, pulse **Siguiente**.

   Consulte la sección Tabla 221 en la página 854 para obtener una descripción de cada uno de los parámetros de configuración.

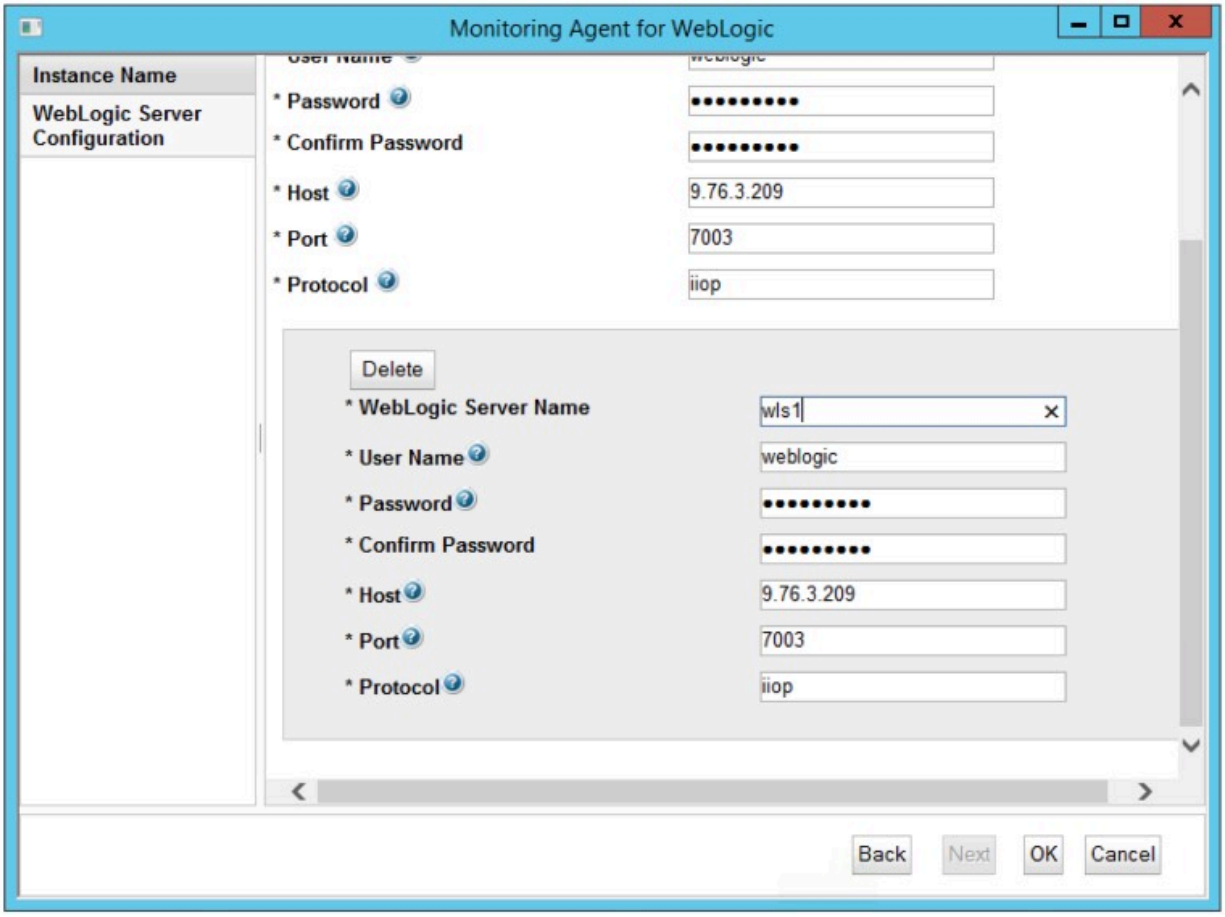


Figura 30. La ventana para especificar valores de instancia de conexión del servidor de WebLogic

7. Pulse **Aceptar** para completar la configuración.
8. Copie los archivos de seguridad de WebLogic en el directorio binario de Agente de WebLogic.
   a. Ubique los archivos `wlclient.jar` y `wljmxclient.jar` bajo `ORACLE_HOME`. Por ejemplo, `C:\Oracle\Middleware\Oracle_Home\wlserver\server\lib`.
   b. Copie los archivos del paso "8.a" en la página 851 en el directorio binario de Agente de WebLogic.
      - Linux AIX *dir_instalación*`/bin`.
      - Windows *dir_instalación*`\TMAITM6_x64`

      donde *dir_instalación* es la vía de acceso donde está instalado el agente. Las vías de acceso de *dir_instalación* predeterminadas se listan aquí:
      - Linux AIX `/opt/ibm/apm/agent`
      - Windows `C:\IBM\APM\TMAITM6_x64`
9. En la ventana IBM Cloud Application Performance Management, pulse con el botón derecho sobre la instancia que ha configurado y pulse **Iniciar**.

Configuración del agente respondiendo a solicitudes

Después de la instalación del Agente de WebLogic, debe configurarlo para poder iniciar el agente. Si el Agente de WebLogic está instalado en un sistema Linux o UNIX local, puede seguir estas instrucciones para configurarlo interactivamente a través de solicitudes de línea de mandatos.

Acerca de esta tarea

Recuerde: Si está volviendo a configurar una instancia de agente configurada, se visualiza el valor que se establece en la última configuración para cada opción. Si desea borrar un valor existente, pulse la tecla de espacio cuando se visualice el valor.

Procedimiento

Siga estos pasos para configurar el Agente de WebLogic ejecutando un script y respondiendo a solicitudes.

1. Ejecute el mandato siguiente.

   dir_instalación/bin/weblogic-agent.sh config **nombre_instancia**

   donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/weblogic-agent.sh config example-inst01
   ```

2. Responda a las solicitudes para establecer valores de configuración para el agente.

   Consulte la sección "Parámetros de configuración para el Agente de WebLogic" en la página 854 para obtener una descripción de cada uno de los parámetros de configuración.

3. Copie los archivos de la biblioteca de cliente de WebLogic en el directorio binario de Agente de WebLogic.

   a) Ubique los archivos `wlclient.jar` y `wljmxclient.jar` bajo `ORACLE_HOME`.

   b) Copie los archivos del paso "3.a" en la página 852 en el directorio binario de Agente de WebLogic.

   dir_instalación/bin

   Donde *dir_instalación* es la vía de acceso donde está instalado el agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin
   ```

4. Ejecute el mandato siguiente para iniciar el agente:

   dir_instalación/bin/weblogic-agent.sh start **nombre_instancia**

   Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

   Ejemplo

   ```
   /opt/ibm/apm/agent/bin/weblogic-agent.sh start example-inst01
   ```

Configuración del agente mediante el archivo de respuestas silencioso

El archivo de respuestas silencioso contiene los parámetros de configuración del agente. Puede editar el archivo de respuestas silencioso para modificar los valores de estos parámetros y ejecutar el script de configuración para crear una instancia y actualizar los valores de configuración de agente. Esta modalidad de configuración se denomina modalidad silenciosa.

Acerca de esta tarea

El archivo de respuestas silencioso contiene los parámetros de configuración del agente con los valores predeterminados definidos para algunos parámetros. Puede editar el archivo de respuestas silencioso para especificar diferentes valores para los parámetros de configuración.

Una vez actualizados los valores de configuración en el archivo de respuestas silencioso, hay que ejecutar el script de configuración para configurar el agente con estos valores actualizados.

Procedimiento

Configure el Agente de WebLogic en modalidad silenciosa siguiendo estos pasos.

1. En un editor de texto, abra el archivo `weblogic_silent_config.txt`, que está disponible en la siguiente vía de acceso:
   - Linux AIX *dir_instalación*`/samples/weblogic_silent_config.txt`
   - Windows *dir_instalación*`\samples\weblogic_silent_config.txt`

   Donde *dir_instalación* es la vía de acceso donde está instalado el agente.

   Ejemplo
   - Linux AIX `/opt/ibm/apm/agent/samples/weblogic_silent_config.txt`
   - Windows `C:\IBM\APM\samples\weblogic_silent_config.txt`
2. En el archivo `weblogic_silent_config.txt` , especifique valores para todos los parámetros obligatorios. También puede modificar los valores predeterminados de otros parámetros.

   Consulte la sección "Parámetros de configuración para el Agente de WebLogic" en la página 854 para obtener una descripción de cada uno de los parámetros de configuración.
3. Guarde y cierre el archivo `weblogic_silent_config.txt` y ejecute el mandato siguiente:
   - Linux AIX *dir_instalación*`/bin/weblogic-agent.sh config` **`nombre_instancia`** *dir_instalación*`/samples/weblogic_silent_config.txt`
   - Windows *dir_instalación*`\bin\weblogic-agent.bat config` **`nombre_instancia`** *dir_instalación*`\samples\weblogic_silent_config.txt`

   donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre que desea dar a la instancia del agente.

   Las vías de acceso de *dir_instalación* predeterminadas se listan aquí:
   - Linux AIX `/opt/ibm/apm/agent`
   - Windows `C:\IBM\APM\TMAITM6_x64`

   Importante: asegúrese de incluir la vía de acceso absoluta al archivo de respuestas silencioso. De lo contrario, los datos de agente no se mostrarán en los paneles de instrumentos.

   Ejemplo
   - Linux AIX `/opt/ibm/apm/agent/bin/weblogic-agent.sh config example-inst01 /opt/ibm/apm/agent/samples/weblogic_silent_config.txt`
   - Windows `C:\IBM\APM\bin\weblogic-agent.bat config example-inst01 C:\IBM\APM\samples\weblogic_silent_config.txt`
4. Copie las bibliotecas de cliente de WebLogic en el directorio binario del Agente de WebLogic.
   a. Ubique los archivos `wlclient.jar` y `wljmxclient.jar` bajo `ORACLE_HOME`.
   b. Copie los archivos del paso "5.a" en la página 853 en el directorio binario de Agente de WebLogic.
      - Linux AIX *dir_instalación*`/bin`.
      - Windows *dir_instalación*`\TMAITM6_x64`

   donde *dir_instalación* es la vía de acceso donde está instalado el agente. Las vías de acceso de *dir_instalación* predeterminadas se listan aquí:
   - Linux AIX `/opt/ibm/apm/agent`
   - Windows `C:\IBM\APM\TMAITM6_x64`
5. Ejecute el mandato siguiente para iniciar el agente:

- Linux AIX *dir_instalación*/bin/weblogic-agent.sh start **nombre_instancia**
- Windows *dir_instalación*\bin\weblogic-agent.bat start **nombre_instancia**

Donde *dir_instalación* es la vía de acceso donde está instalado el agente y *nombre_instancia* es el nombre de la instancia de agente.

Las vías de acceso de *dir_instalación* predeterminadas se listan aquí:

- Linux AIX /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

Ejemplo

- Linux AIX /opt/ibm/apm/agent/bin/weblogic-agent.sh start example-inst01
- Windows C:\IBM\APM\bin\weblogic-agent.bat start example-inst01

Parámetros de configuración para el Agente de WebLogic

Los parámetros de configuración del Agente de WebLogic se visualizan en una tabla.

1. Valores del agente de WebLogic - Valores de entorno del agente de WebLogic.

Tabla 221. Valores del agente de WebLogic

Nombre de parámetro	Descripción	Nombre de parámetro del archivo de configuración silenciosa
Nombre de servidor de WebLogic	Proporcione un nombre para identificar la instancia de agente del servidor de WebLogic. Ejemplo: *wls1* **Nota:** este alias puede ser cualquier cosa que elija para representar la instancia de agente de servidor de WebLogic, con las limitaciones siguientes. Sólo se pueden utilizar letras, números arábigos, el carácter de subrayado y el símbolo "menos" en el nombre de la conexión. La longitud máxima de un nombre de conexión son 25 caracteres.	Cada uno de los parámetros siguientes debe tener un sufijo de nombre de instancia que será el mismo para cada parámetro de una instancia de agente. Las instancias de agente nuevas deben utilizar un nombre de instancia exclusivo para su conjunto de parámetros. Por ejemplo, una instancia de agente puede utilizar *.wls1* y otra instancia del agente puede utilizar *.wls*2 en lugar de *.nombre_instancia* en los nombres de parámetro siguientes.
Nombre de usuario	Nombre de usuario utilizado para autenticar con el servidor de WebLogic.	**KWB_WLS_USERNAME.nombre_instancia**
Contraseña	Contraseña utilizada para autenticar con el servidor de WebLogic.	**KWB_WLS_PASSWORD.nombre_instancia**
Host	Host utilizado para autenticar con el servidor de WebLogic. Escriba el nombre de host completo o la dirección IP del servidor de WebLogic.	**KWB_WLS_HOST.nombre_instancia**
Puerto	Puerto utilizado para autenticar con el servidor de WebLogic.	**KWB_WLS_PORT.nombre_instancia**
Protocolo	Protocolo utilizado para autenticar con el servidor de WebLogic. Se da soporte a los protocolos *iiop* y *https*.	**KWB_WLS_PROTOCOL.nombre_instancia**

Configuración del rastreo de transacciones para el Agente de WebLogic

La prestación de rastro de transacciones del Agente de WebLogic requiere cambios en el archivo de valores de entorno de instancia de agente y en el archivo de arranque del servidor WebLogic. Se proporciona un script para ayudarle a hacer los cambios.

Antes de empezar

Linux AIX Asegúrese de que el límite de recursos para archivos abiertos es mayor que 5.000 para que el kit de herramientas de rastreo de transacciones funcione adecuadamente.

- Muestra el valor límite de archivos abiertos actual. **`ulimit -n`**
- Ejemplo que establece el límite de archivos abiertos en 5.056. **`ulimit -n 5056`**

Ejecute el procedimiento "Configuración de la supervisión de WebLogic" en la página 846 Windows paso 1 o Linux AIX paso 2 antes de seguir este procedimiento.

Nota: La prestación de rastreo de transacciones está disponible para el Agente de WebLogic en la oferta Cloud APM, Advanced. Para el Agente de WebLogic con prestación de supervisión de recursos básica, que se encuentra en la oferta Cloud APM, Base, omita este paso.

El Agente de WebLogic debe estar instalado localmente en el servidor WebLogic supervisado con la prestación de rastreo de transacciones.

La cuenta de usuario que ejecuta este script debe tener permiso de escritura sobre los directorios y archivos siguientes:

1. El directorio *WEBLOGIC_HOME*.
2. El directorio y los archivos de *WEBLOGIC_HOME*`/bin`.
3. El directorio *dir_instalación*`/config`.
4. El archivo *dir_instalación*`/config/`*nombre_host*`_wb_`*nombre_instancia*`.cfg`.

donde

WEBLOGIC_HOME
Directorio de instalación del servidor WebLogic.

dir_instalación
Vía de acceso donde está instalado el agente. Las vías de acceso predeterminadas a estos registros son las siguientes.

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

nombreHost
Nombre del sistema principal en el que se instala el agente.

nombre_instancia
Nombre de la instancia de agente asignada en el tema de método de configuración de agente:

- Configuración del agente en sistemas Windows, paso "3" en la página 848
- Configuración del agente respondiendo a solicitudes, paso "1" en la página 852
- Configuración del agente mediante el archivo de respuestas silencioso, paso "2" en la página 853

Procedimiento

Ejecute el script **`simpleConfig`**.

1. Inicie la sesión en el servidor WebLogic con el Agente de WebLogic instalado.
2. Vaya al directorio de instalación del agente.
   - Linux AIX *dir_instalación*

- Windows *dir_instalación*\TMAITM6_x64

Donde *dir_instalación* es la vía de acceso donde está instalado el agente.

Las vías de acceso de *dir_instalación* predeterminadas se listan aquí:

- Linux AIX /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

3. Vaya al directorio wbdchome/8.1.4.0.0/bin.
4. Ejecute el script de configuración.
   - Linux AIX ./simpleConfig.sh
   - Windows simpleConfig.bat
5. Siga las indicaciones para especificar parámetros para su entorno:
   a) Elija el *nombre_instancia* y el subnodo del Agente de WebLogic para la configuración en la lista de combinaciones de instancias de agente y subnodos detectados, donde *nombre_instancia* es el nombre de la instancia de agente.
   b) Escriba el número del método de arranque del servidor WebLogic.
   c) Escriba la vía de acceso de búsqueda raíz del dominio de WebLogic.
      Esta vía de acceso se utiliza como la base desde la que realizar búsquedas en dominios de WebLogic. Si la variable de entorno *WEBLOGIC_HOME* está establecida, el valor correspondiente se ofrece como el valor predeterminado.
   d) Escriba el número del dominio WebLogic del servidor WebLogic a configurar.
   e) Escriba el número del nombre del servidor WebLogic a configurar.

Linux Configuración de ejemplo con un método de arranque de WebLogic de Script de inicio de WebLogic.

```
./simpleconfig.sh

Los agentes y subnodos siguientes no están configurados todavía para el rastreo de
transacciones:

1) wlinst1 Server1
2) wlinst1 Server2

Escriba el número que corresponde a la instancia y el subnodo de agente que desea configurar.

Escriba aquí su selección (por ejemplo: 1): 1

Se da soporte a los métodos de arranque de WebLogic siguientes:

1) Script de inicio de WebLogic
2) Gestor de nodos de WebLogic

Escriba aquí su selección (el valor predeterminado es 1): 1

La vía de acceso para empezar a buscar dominios de WebLogic.
Raíz de la búsqueda de dominios de WebLogic (el valor predeterminado es: ): /home/wlsadmin

Las vías de acceso de dominio de WebLogic encontradas son:

1) /home/wlsadmin/oracle/user_projects/domains/ttdd

Escriba el número correspondiente al dominio de WebLogic que contiene el servidor de
WebLogic que desea configurar.

Escriba aquí la selección (por ejemplo: 1): 1

Los servidores WebLogic siguientes están disponibles para configuración:

1) AdminServer
2) Server1

Seleccione un nombre de servidor de WebLogic (el valor predeterminado es: 2): 2
INFO: [2000] La configuración automática del archivo de entorno de agente ha sido
satisfactoria.
INFO: [3000] La configuración automática del script de inicio de WebLogic ha sido
```

```
satisfactoria.
INFO: [9000] Reinicie el agente de WebLogic y el servidor de WebLogic para que la
configuración
entren en vigor.
```

6. Siga estos pasos si se ha seleccionado `Gestor de nodos de WebLogic` se ha seleccionado como **`Método de arranque de servidor WebLogic`** en el paso "5.b" en la página 856. De lo contrario, continúe con el paso "7" en la página 858.
   a) Abra el archivo `weblogic_nodemanager_dc_opts` que se lista en el mensaje de información número 3011 del texto de salida del paso "5" en la página 856.

      Windows Salida de configuración de ejemplo con un método de arranque de WebLogic de `Gestor de nodos de WebLogic`.

      ```
      INFO: [2000] La configuración automática del archivo de entorno de agente ha sido
      satisfactoria.
      INFO: [3010] La configuración automática del script de inicio de WebLogic se ha saltado.
      INFO: [3011] Revise C:\IBM\APM\TMAITM6_x64\wbdchome\8.1.4.0.0\runtime\ttdd_win
      \win_Server1\
      staging\weblogic_nodemanager_dc_opts.win para conocer las opciones de inicio de máquina
      virtual Java de WebLogic necesarias.
      INFO: [9000] Reinicie el agente de WebLogic y el servidor de WebLogic para que la
      configuración
      entren en vigor.
      ```

   b) Inicie la sesión en la consola de WebLogic y seleccione **Entorno** > **Servidores**.
   c) Seleccione el servidor a configurar.
   d) Seleccione la pestaña **Configuración** > **Inicio de servidor**.
   e) Copie los argumentos de inicio de servidor del archivo `weblogic_nodemanager_dc_opts` a los argumentos de **Inicio de servidor** del servidor en la consola WebLogic y guarde los cambios.

      Los argumentos de inicio de servidor son todas las líneas que siguen a la línea de comentario `# Añada las líneas siguientes a los argumentos de inicio de servidor` en el archivo `weblogic_nodemanager_dc_opts`.
   f) Asegúrese de que el kit de herramientas de rastreo de transacción está en la vía de acceso de biblioteca compartida durante el tiempo de ejecución.

      Elija un método.

      - Actualice el script de inicio del Gestor de nodos.

        Nota: Todos los servidores de WebLogic iniciados por el Gestor de nodos tienen esta vía de acceso de bibliotecas establecida con las bibliotecas de archivo de objeto de kit de herramientas de transacción incluidas.

        1) Abra el archivo `weblogic_nodemanager_dc_opts` que se lista en el mensaje de información número 3011 del texto de salida del paso "5" en la página 856.
        2) Establezca la vía de acceso del kit de herramientas de rastreo de transacciones en el script de inicio del Gestor de nodos. El mandato para establecer la vía de acceso es la línea que sigue a la línea de comentario `# Asegúrese de que la vía de acceso ejecutable disponible para el servidor de WebLogic incluye el directorio lib del kit de herramientas` en el archivo `weblogic_nodemanager_dc_opts`.

           – Linux Copie la línea LD_LIBRARY_PATH del archivo `weblogic_nodemanager_dc_opts.linux` generado y péguela bajo la línea `export JAVA_OPTIONS` en el script de inicio del Gestor de nodos. Por ejemplo, *`WEBLOGIC_HOME`*`/user_projects/domains/`*`nombre_dominio`*`/bin/startNodeManager.sh`.

           – Windows Copie la línea PATH del archivo `weblogic_nodemanager_dc_opts.win` generado y péguela bajo la línea `export JAVA_OPTIONS` del script de inicio del Gestor de nodos. Por ejemplo, *`WEBLOGIC_HOME`*`\user_projects\domains\`*`nombre_dominio`*`\bin\startNodeManager.bat`.

        donde *WEBLOGIC_HOME* es el directorio de instalación del servidor WebLogic y *nombre_dominio* es el nombre del dominio de WebLogic.

- Actualice el entorno de la cuenta de usuario que inicia el Gestor de nodos.

  Nota: Todas las aplicaciones iniciadas por la cuenta de usuario tienen esta vía de acceso de biblioteca establecida con las bibliotecas de archivo de objeto de kit de herramientas incluidas.

  1) Edite los valores de entorno para el usuario que inicia el Gestor de nodos.

     – Linux AIX Edite el archivo de recursos de shell o el archivo de perfil de shell. Por ejemplo, en el shell bash, `.bashrc` o `.bash_profile`.

     – Windows Edite **Panel de control** > **Seguridad y sistema** > **Sistema** > **Valores avanzados del sistema** > **Variables de entorno...** > **Variables de usuario para *nombre_usuario*** > **Path**, donde *nombre_usuario* es el nombre de la cuenta de usuario utilizada para iniciar el servidor WebLogic.

  2) Establezca la vía de acceso del kit de herramientas de rastreo de transacciones en el entorno de cuenta de usuario. El mandato para establecer la vía de acceso es la línea que sigue a la línea de comentario `# Asegúrese de que la vía de acceso ejecutable disponible para el servidor de WebLogic incluye el directorio lib del kit de herramientas` en el archivo `weblogic_nodemanager_dc_opts`.

     – Linux AIX Copie la línea `export LD_LIBRARY_PATH` del archivo `weblogic_nodemanager_dc_opts.linux` generado. Si una línea de `export LD_LIBRARY_PATH` no existe, añádala. Si existe, edítela para añadir solo la vía de acceso desde la derecha del signo igual a la vía de acceso existente con el delimitador de vía de acceso correcto.

     – Windows Copie la línea `set PATH` del archivo `weblogic_nodemanager_dc_opts.win` generado. Si una variable **Path** no existe en la sección **Variables de usuario para *nombre_usuario***, donde *nombre_usuario* es el nombre de la cuenta de usuario utilizada para iniciar el servidor WebLogic, añádala especificando `Path` como el nombre de variable y la vía de acceso desde la derecha del signo igual como valor. Si existe, edite el valor para añadir solo la vía de acceso desde la derecha del signo igual a la vía de acceso existente con el delimitador de vía de acceso correcto.

  3) Vuelva a cargar el entorno.

  Aviso: El programa de utilidad de configuración de WebLogic genera los scripts de `startNodeManager`. Por lo tanto, puede perder los cambios cuando se vuelve a ejecutar la configuración de WebLogic.

7. Si el servidor y el agente de WebLogic se están ejecutando, reinícielos.

Resultados

Archivos de servidor WebLogic cambiados durante la configuración del rastreo de transacciones:

- El script `startManagedWebLogic`.
  – Linux AIX *WEBLOGIC_HOME*`/bin/startManagedWebLogic.sh`
  – Windows *WEBLOGIC_HOME*`\bin\startManagedWebLogic.cmd`

  Donde *WEBLOGIC_HOME* es el directorio de instalación del servidor WebLogic.

  Este archivo se actualiza con los valores de configuración para la prestación de rastreo de transacciones. Los marcadores de configuración se insertan en el archivo para utilizarlos al inhabilitar la prestación de rastreo de transacciones. Se guarda un archivo de copia de seguridad en el directorio *WEBLOGIC_HOME*`/bin/bak/` antes de que el script añada o elimine los cambios de prestación de rastreo de transacciones.

Archivos de agente cambiados durante la configuración del rastreo de transacciones:

- Archivo de configuración de instancia de agente
  – Linux AIX *dir_instalación*`/config/`*nombre_host*`_wb_`*nombre_instancia*`.cfg`

– Windows *dir_instalación*\TMAITM6_x64*nombre_host*_WB_*nombre_instancia*.cfg

- Archivo de valores de entorno de agente
  – Linux AIX *dir_instalación*/config/wb_*nombre_instancia*.environment
  – Windows *dir_instalación*\TMAITM6_x64\KWBENV_*nombre_instancia*

donde

dir_instalación
Vía de acceso donde está instalado el agente. Las vías de acceso predeterminadas a estos registros son las siguientes.

- Linux AIX /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

nombreHost
Nombre del sistema principal en el que se instala el agente.

nombre_instancia
Nombre de la instancia de agente asignada en el tema de método de configuración de agente:

- Configuración del agente en sistemas Windows, paso "3" en la página 848
- Configuración del agente respondiendo a solicitudes, paso "1" en la página 852
- Configuración del agente mediante el archivo de respuestas silencioso, paso "2" en la página 853

Inhabilitación del rastreo de transacciones para una instancia del Agente de WebLogic
La prestación de rastreo de transacciones del Agente de WebLogic se puede eliminar. Se proporciona un script para eliminar la prestación de rastreo de transacciones para una instancia de agente.

Antes de empezar

Asegúrese de haber concluido el servidor WebLogic y el Agente de WebLogic.

La cuenta de usuario que ejecuta este script debe tener permiso de escritura sobre los directorios y archivos siguientes:

1. El directorio *WEBLOGIC_HOME*.
2. El directorio y los archivos de *WEBLOGIC_HOME*/bin.
3. El directorio *dir_instalación*/config.
4. El archivo *dir_instalación*/config/*nombre_host*_wb_*nombre_instancia*.cfg.

Procedimiento

Ejecute el script **unconfig** con la opción **remove**.

1. Inicie la sesión en el servidor WebLogic con el Agente de WebLogic instalado.
2. Vaya al directorio de instalación del agente.
   - Linux AIX *dir_instalación*
   - Windows *dir_instalación*\TMAITM6_x64
3. Vaya al directorio wbdchome/8.1.4.0.0/bin.
4. Ejecute **unconfig** con la opción **remove** y el nombre de instancia y de subnodo de agente.
   - Para inhabilitar un subnodo de una instancia de agente, utilice el parámetro *subnode_name*.
     – Linux AIX ./unconfig.sh **remove** *instance_name subnode_name*
     – Windows unconfig.bat **remove** *instance_name subnode_name*
   - Para inhabilitar todos los subnodos para una instancia de agente, omita el parámetro *subnode_name*.

- Linux AIX `./unconfig.sh` **`remove`** *`instance_name`*
- Windows `unconfig.bat` **`remove`** *`instance_name`*

5. Inicie el servidor WebLogic y el agente.

donde

WEBLOGIC_HOME
Directorio de instalación del servidor WebLogic.

nombreHost
Nombre del sistema principal en el que se instala el agente.

nombre_instancia
Nombre de la instancia de agente asignada en el tema de método de configuración de agente:

- Configuración del agente en sistemas Windows, paso "3" en la página 848
- Configuración del agente respondiendo a solicitudes, paso "1" en la página 852
- Configuración del agente mediante el archivo de respuestas silencioso, paso "2" en la página 853

nombre_subnodo
Nombre del subnodo de instancia de agente asignado al parámetro **Nombre del servidor de WebLogic** en el tema de método de configuración de agente:

- Configuración del agente en sistemas Windows, paso "6" en la página 850
- Configuración del agente respondiendo a solicitudes, paso "2" en la página 852
- Configuración del agente mediante el archivo de respuestas silencioso, paso "2" en la página 853

dir_instalación
Vía de acceso donde está instalado el agente. Las vías de acceso predeterminadas a estos registros son las siguientes.

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

Desinstalación del rastreo de transacciones para el Agente de WebLogic
La prestación de rastreo de transacciones de Agente de WebLogic se puede desinstalar. Se proporciona un script para eliminar la prestación de rastreo de transacciones de todas las instancias de agente y también para eliminar el kit de herramientas de rastreo de transacciones.

Antes de empezar

Asegúrese de que haber concluido el servidor WebLogic y todas las instancias del Agente de WebLogic.

La cuenta de usuario que ejecuta este script debe tener permiso de escritura sobre los directorios y archivos siguientes:

1. El directorio *`WEBLOGIC_HOME`*.
2. El directorio y los archivos de *`WEBLOGIC_HOME`*`/bin`.
3. El directorio *`dir_instalación`*`/config`.
4. El archivo *`dir_instalación`*`/config/`*`nombre_host`*`_wb_`*`nombre_instancia`*`.cfg`.

Procedimiento

Ejecute el script **`unconfig`** con la opción **`uninstall`**.

1. Inicie la sesión en el servidor WebLogic con el Agente de WebLogic instalado.
2. Vaya al directorio de instalación del agente.

- Linux AIX *`dir_instalación`*

- Windows *dir_instalación*\TMAITM6_x64

3. Vaya al directorio wbdchome/8.1.4.0.0/bin.
4. Ejecute **unconfig** con la opción **uninstall**.
   - Linux AIX ./unconfig.sh **uninstall**
   - Windows unconfig.bat **uninstall**
5. Inicie el servidor WebLogic y todas las instancias de agente.

   donde

   WEBLOGIC_HOME
   Directorio de instalación del servidor WebLogic.

   nombreHost
   Nombre del sistema principal en el que se instala el agente.

   nombre_instancia
   Nombre de la instancia de agente asignada en el tema de método de configuración de agente:
   - Configuración del agente en sistemas Windows, paso "3" en la página 848
   - Configuración del agente respondiendo a solicitudes, paso "1" en la página 852
   - Configuración del agente mediante el archivo de respuestas silencioso, paso "2" en la página 853

   dir_instalación
   Vía de acceso donde está instalado el agente. Las vías de acceso predeterminadas a estos registros son las siguientes.
   - Linux AIX /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64

Configuración del Panel de instrumentos del rendimiento de aplicaciones para visualizar datos de rastreo de transacciones para el Agente de WebLogic

La visualización de datos recopilados por la prestación de rastreo de transacciones del Agente de WebLogic requiere la realización de cambios de configuración en el Panel de instrumentos del rendimiento de aplicaciones.

Antes de empezar

Realice la "Configuración del rastreo de transacciones para el Agente de WebLogic" en la página 855 antes de seguir este procedimiento.

Procedimiento

1. Habilite los datos de rastreo de transacciones en Panel de instrumentos del rendimiento de aplicaciones si tiene Agente de WebLogic con prestación de rastreo, que se encuentra en la oferta Cloud APM, Advanced y desea habilitar la prestación de rastreo de transacciones.
   a) En la barra de navegación, pulse **Configuración del sistema** > **Configuración del agente**.
   Se mostrará la página **Configuración del agente**.
   b) Seleccione la pestaña **WebLogic**.
   c) Seleccione los recuadros de selección correspondientes a las instancias de agente del servidor WebLogic que desea supervisar y lleve a cabo una de las acciones siguientes de la lista **Acciones**:
   - Para habilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Habilitado**. El estado de la columna **Rastreo de transacciones** se actualizará a *Habilitado*.
   - Para inhabilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Inhabilitado**. El estado de la columna **Rastreo de transacciones** se actualiza a *Inhabilitado*.

2. para ver los paneles de instrumentos de datos de rastreo de transacciones del Agente de WebLogic, añada la instancia del Agente de WebLogic a una aplicación en el Panel de instrumentos del rendimiento de aplicaciones.

   Para obtener más información sobre el editor de aplicaciones, consulte Gestión de aplicaciones.
3. Asegúrese de que las cuentas de usuario están asignadas a un rol que incluya el permiso de panel de instrumentos de diagnóstico para tener acceso a los siguientes botones del Panel de instrumentos de aplicaciones de rastreo de transacciones del Agente de WebLogic.

   De lo contrario, estos botones están inhabilitados para ese usuario en el Panel de instrumentos de aplicaciones.

   a. El botón detallado **Diagnosticar** del widget **5 Tiempos de respuesta más lentos**.

   b. El botón **Solicitudes en curso** del widget **Aplicaciones**.

Configuración de la supervisión de WebSphere Applications

La configuración de la supervisión de WebSphere Applications implica la configuración de un recopilador de datos para los servidores de aplicaciones. El recopilador de datos puede ser autónomo o incorporado con el Agente de WebSphere Applications.

Recopilador de datos incorporado

La mayoría de los servidores de aplicaciones de WebSphere se pueden supervisar mediante el recopilador de datos incorporado, excepto el perfil de Liberty en IBM Cloud. El recopilador de datos incorporado puede proporcionar todas las características de supervisión.

Para configurar el recopilador de datos incorporado, primero debe instalar el Agente de WebSphere Applications en el sistema en el que el servidor de aplicaciones se está ejecutando. Después de eso, utilice los programas de utilidad de configuración proporcionados para configurar el recopilador de datos de forma interactiva o silenciosa.

Recopilador de datos autónomo

El recopilador de datos autónomo solo es aplicable a WebSphere Application Server Liberty on Linux for System x y al perfil de WebSphere Liberty en IBM Cloud.

Si opta por configurar un recopilador de datos autónomo, puede saltarse el procedimiento de instalación del agente y configurar directamente el recopilador de datos en Liberty.

Sin embargo, el recopilador de datos autónomo no recopilará algunos datos de diagnóstico como por ejemplo el vuelco de almacenamiento dinámico en el momento actual o la información de solicitudes en curso. Esto significa que sólo puede habilitar el recopilador de datos para recopilar automáticamente información de vuelco de almacenamiento dinámico a intervalos especificados, pero no puede tomar instantáneas de almacenamiento dinámico siempre que desee utilizando el botón **Tomar instantánea** de la Consola de Cloud APM. No todos los paneles de instrumentos relacionados con solicitudes en curso, que el recopilador de datos incorporado puede suministrar, están disponibles para el recopilador de datos autónomo.

Utilice Tabla 222 en la página 862 para determinar el recopilador de datos adecuado para su servidor de aplicaciones.

Tabla 222. Aplicaciones WebSphere y recopiladores de datos aplicables

Aplicación a supervisar	Recopilador de datos aplicable	Documentación
WebSphere Application Server tradicional	Recopilador de datos incorporado	“Configuración del recopilador de datos para Agente de WebSphere Applications” en la página 863

Tabla 222. Aplicaciones WebSphere y recopiladores de datos aplicables (continuación)		
Aplicación a supervisar	**Recopilador de datos aplicable**	**Documentación**
WebSphere Application Server Liberty (local)	• Recopilador de datos incorporado • Recopilador de datos autónomo (solo Linux for System x)	• "Configuración del recopilador de datos para Agente de WebSphere Applications" en la página 863 • "Configuración del recopilador de datos para aplicaciones locales" en la página 912
Perfil WebSphere Liberty en IBM Cloud	Recopilador de datos autónomo	"Configuración del recopilador de datos de Liberty para aplicaciones IBM Cloud" en la página 916
Perfil WebSphere Liberty en contenedor Docker	Recopilador de datos incorporado	"Supervisión de WebSphere Application Server Liberty dentro de un contenedor de Docker" en la página 898

Configuración del recopilador de datos para Agente de WebSphere Applications

El Agente de WebSphere Applications no necesita ninguna configuración tras la instalación del agente, a menos que desee cambiar el puerto predeterminado. Sin embargo, debe configurar el recopilador de datos, que es un componente del agente, para configurar la supervisión del entorno WebSphere.

Acerca de esta tarea

Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.

Procedimiento

- (Método rápido) Si sólo utiliza el Agente de WebSphere Applications sin el producto de herencia ITCAM Agent for WebSphere Applications en el entorno, para configurar la supervisión con rapidez, consulte "Pista rápida: Configuración del recopilador de datos para el Agente de WebSphere Applications" en la página 864 para obtener un flujo de configuración simplificado.
- (Configuración simple) Para un flujo de configuración completo en un entorno puro de IBM Cloud Application Performance Management, consulte "Configuración del recopilador de datos con el programa de utilidad de configuración simple" en la página 867.
- (Configuración completa) Para configurar el recopilador de datos con más opciones de personalización, utilice los programas de utilidad de configuración completa. Para obtener instrucciones, consulte "Configuración o reconfiguración del recopilador de datos con los programas de utilidad de configuración completa" en la página 869.
- (Configuración silenciosa) Para desplegar la misma supervisión para varias instancias de servidor de aplicaciones, configure el recopilador de datos en modalidad silenciosa. Para obtener instrucciones, consulte "Configuración del recopilador de datos en modalidad silenciosa" en la página 878.
- (WebSphere Portal Server) Para supervisar instancias de WebSphere Portal Server, utilice el procedimiento de configuración avanzada. Para obtener instrucciones, consulte "Configuración o reconfiguración del recopilador de datos con los programas de utilidad de configuración completa" en la página 869.
- (Configuración manual) Si no puede utilizar los programas de utilidad de configuración suministrados para configurar el recopilador de datos para el Agente de WebSphere Applications, configure manualmente el recopilador de datos en WebSphere Administrative Console. Para obtener

instrucciones, consulte "Configuración manual del recopilador de datos si fallan los programas de utilidad de configuración" en la página 886.

- (Coexistencia de agentes) Si desea configurar el recopilador de datos para que funcione en un entorno de coexistencia de agentes en el que están instalados el Agente de WebSphere Applications e ITCAM Agent for WebSphere Applications, consulte la sección "(Coexistencia de agentes) Configuración del Agente de WebSphere Applications y del recopilador de datos" en la página 890.
- (Supervisión de Docker) Para supervisar WebSphere Application Server Liberty ejecutado dentro de un contenedor de Docker, consulte "Supervisión de WebSphere Application Server Liberty dentro de un contenedor de Docker" en la página 898.

Pista rápida: Configuración del recopilador de datos para el Agente de WebSphere Applications
El Agente de WebSphere Applications no necesita ninguna configuración tras la instalación del agente. Sin embargo, debe configurar el recopilador de datos, que es un componente del agente, para configurar la supervisión del entorno WebSphere.

Antes de empezar

1. Instale el Agente de WebSphere Applications en el sistema en el que el servidor de aplicaciones que debe supervisarse está instalado y en ejecución.
2. Compruebe los requisitos de acceso de usuario.
   - Windows Utilice el ID de administrador que se utiliza para instalar el servidor de aplicaciones para configurar el recopilador de datos. Asegúrese de que este ID de usuario tenga permiso de escritura completo sobre el directorio de inicio del recopilador de datos, *dir_instalación*\dchome\7.3.0.14.08.
   - Linux AIX Utilice el ID de usuario que se ha utilizado para instalar el servidor de aplicaciones para configurar el recopilador de datos. Asegúrese de que este ID de usuario tiene permisos de lectura y escritura sobre los directorios siguientes de *dir_instalación*/yndchome/7.3.0.14.08:
     - bin
     - data
     - runtime

Acerca de esta tarea

En este procedimiento se utiliza un programa de utilidad de configuración simple, `simpleconfig`, para suministrar la configuración básica del recopilador de datos.

El programa de utilidad `simpleconfig` configura el recopilador de datos con valores predeterminados. Para configurar el recopilador de datos con más opciones de personalización, utilice el programa de utilidad de configuración completa, `config`, en el mismo directorio. Para obtener instrucciones, consulte "Configuración o reconfiguración del recopilador de datos con los programas de utilidad de configuración completa" en la página 869.

En la mayoría de los casos, el programa de utilidad `simpleconfig` es suficiente. En entornos más complejos, puede utilizar el programa de utilidad de configuración `config` para configurar el recopilador de datos. Si el programa de utilidad `simpleconfig` falla, utilice el programa de utilidad `config` en su lugar.

Procedimiento

1. Inicie la sesión en el sistema con el ID de usuario utilizado para instalar el servidor de aplicaciones.
2. Cambie al directorio `bin` del directorio de inicio del recopilador de datos.
   - Windows *dir_instalación*\dchome\7.3.0.14.08\bin
   - Linux AIX *dir_instalación*/yndchome/7.3.0.14.08/bin

3. Ejecute el siguiente programa de utilidad de configuración simple:
   - Windows **simpleconfig.bat**
   - Linux AIX **./simpleconfig.sh**
4. Siga las solicitudes para continuar con la configuración del recopilador de datos.

   Será necesario que realice algunas de las siguientes acciones o todas ellas, en función de los valores del servidor de aplicaciones:

   - Para WebSphere Application Server tradicional:
     - Seleccione el directorio de instalación de WebSphere descubierto automáticamente o especifique manualmente el directorio de instalación.
     - Seleccione el perfil de WebSphere Application Server para supervisar.
     - Seleccione el perfil de propiedades de seguridad que debe utilizarse o proporcione el nombre de usuario y la contraseña de la consola de administración de WebSphere (si la seguridad está habilitada para el servidor de aplicaciones).
   - Para WebSphere Application Server Liberty:
     - Especifique la vía de acceso completa del directorio inicial de Liberty que contiene los directorios `bin` y `servers`. Por ejemplo, `/opt/ibm/wlp`.
     - Especifique el directorio inicial del JRE utilizado por Liberty.
5. Una vez finalizada la configuración del recopilador de datos, reinicie el servidor de aplicaciones.
   a) Vaya al directorio `bin` bajo el directorio de inicio del perfil de servidor de aplicaciones. Por ejemplo, `opt/IBM/WebSphere/AppServer/profiles/`*`nombre_perfil`*`/bin`.
   b) Detenga el servidor de aplicaciones especificando el mandato **stopServer** en la consola de mandatos.
      - Linux AIX `./stopServer.sh` *`nombre_servidor`*
      - Windows `stopServer.bat` *`nombre_servidor`*
   c) Cuando se le solicite, especifique el ID de usuario y la contraseña del administrador de la consola de administración de WebSphere.
   d) Inicie de nuevo el servidor de aplicaciones especificando el mandato **startServer** en la consola de mandatos.
      - Linux AIX `./startServer.sh` *`nombre_servidor`*
      - Windows `startServer.bat` *`nombre_servidor`*
6. Inicie la sesión en Consola de Cloud APM para ver los datos en los paneles de instrumentos.
   a) Acceda a la consola mediante el enlace que se proporciona en el correo electrónico que le informa de que el servicio está preparado. También puede acceder a la consola desde el sitio web IBM Marketplace. Para obtener instrucciones detalladas, consulte “Inicio de la Consola de Cloud APM” en la página 1009.
   b) Utilice el editor de aplicaciones para añadir el servidor de aplicaciones supervisado al Panel de instrumentos del rendimiento de aplicaciones. Puede añadirlo como componente nuevo a la aplicación existente o crear una aplicación para que contenga este componente.

      Para obtener más información sobre el editor de aplicaciones, consulte “Gestión de aplicaciones” en la página 1133.

Resultados

El recopilador de datos se ha configurado para supervisar la instancia del servidor de aplicaciones. Recuerde que la recopilación de datos puede aumentar la sobrecarga del servidor de aplicaciones. Puede controlar la recopilación de datos con opciones de configuración más avanzadas para el ajuste.

Comprobación de los requisitos de acceso de usuario

El Agente de WebSphere Applications tiene algunos requisitos de acceso para el ID de usuario que debe configurar el recopilador de datos.

Acerca de esta tarea

Utilice el ID que se ha utilizado para instalar el servidor de aplicaciones para configurar el recopilador de datos después de otorgar los permisos adecuados para el ID de instalación del servidor de aplicaciones.

Procedimiento

- Windows Utilice el ID de administrador que se utiliza para instalar el servidor de aplicaciones para configurar el recopilador de datos. Asegúrese de que este ID de usuario tenga permiso de escritura completo sobre el directorio de inicio del recopilador de datos, *dir_instalación*\dchome\7.3.0.14.08.
- Linux AIX Utilice el ID de usuario que se ha utilizado para instalar el servidor de aplicaciones para configurar el recopilador de datos. Asegúrese de que este ID de usuario tiene permisos de lectura y escritura sobre los directorios siguientes de *dir_instalación*/yndchome/7.3.0.14.08:
  - bin
  - data
  - logs
  - runtime

  Recuerde: si utiliza IDs de usuario diferentes para instalar los servidores de aplicaciones, puede que necesite utilizar IDs de usuario diferentes para configurar el recopilador de datos. Después de configurar el recopilador de datos por primera vez, otorgue el permiso de escritura a los archivos siguientes cada vez que utilice un ID de usuario diferente para configurar el recopilador de datos, donde *nombre_perfil* es el nombre de perfil de servidor de aplicaciones:
  - *dir_instalación*/yndchome/7.3.0.14.08/data/findservers.inputlist
  - *dir_instalación*/yndchome/7.3.0.14.08/data/*nombre_perfil*.findservers.progress
  - *dir_instalación*/yndchome/7.3.0.14.08/data/config_inputlist
  - *dir_instalación*/yndchome/7.3.0.14.08/runtime/custom/connections.properties

Manejo de otros recopiladores de datos existentes en el servidor de aplicaciones

Si un recopilador de datos ya existe en el servidor de aplicaciones, debe decidir qué hacer con el recopilador de datos existente, de modo que no entre en conflicto con el recopilador de datos del Agente de WebSphere Applications.

Acerca de esta tarea

Los siguientes tipos de recopiladores de datos ya pueden existen en el servidor de aplicaciones que se va a supervisar:

- El recopilador de datos del Agente de WebSphere Applications, que se instala en una versión anterior de IBM Cloud Application Performance Management
- El recopilador de datos de ITCAM Agent for WebSphere Applications, que se instala en la infraestructura de IBM® Tivoli® Monitoring antigua
- Cualquier otro recopilador de datos no suministrado por IBM

Procedimiento

Realice las acciones adecuadas para evitar conflictos de recopilador de datos.

- Para una versión anterior del recopilador de datos del Agente de WebSphere Applications , que se instala en una versión anterior de IBM Cloud Application Performance Management, tiene las siguientes opciones:
  - Migrar el recopilador de datos con el programa de utilidad de migración desde el directorio de inicio más reciente del recopilador de datos. Para obtener instrucciones, consulte "Agente de WebSphere Applications: Migración del recopilador de datos" en la página 1181.
  - Desconfigurar la versión anterior del recopilador de datos y después configurar el recopilador de datos de nuevo con el programa de utilidad de configuración desde el directorio de inicio más reciente del recopilador de datos. Para obtener información sobre cómo desconfigurar el recopilador de datos, consulte "Agente de WebSphere Applications: Desconfiguración del recopilador de datos" en la página 154.
- Para el recopilador de datos de ITCAM Agent for WebSphere Applications, siga estos pasos si desea desplegar la supervisión en un entorno de coexistencia de agentes:
  a) Desinstale el recopilador de datos de ITCAM Agent for WebSphere Applications.
  b) Configure sólo un recopilador de datos para enviar datos al Agente de WebSphere Applications y a ITCAM Agent for WebSphere Applications. Para obtener instrucciones, consulte "(Coexistencia de agentes) Configuración del Agente de WebSphere Applications y del recopilador de datos" en la página 890.
- En el caso de otros recopiladores de datos no suministrados por IBM, evalúe si es necesario eliminarlos. El recopilador de datos del Agente de WebSphere Applications utiliza la manipulación del código de bytes Java para recopilar datos. Otros recopiladores de datos que utilicen la misma forma de recopilar datos pueden entrar en conflicto con el recopilador de datos de Agente de WebSphere Applications.

Configuración del recopilador de datos con el programa de utilidad de configuración simple
El Agente de WebSphere Applications se inicia automáticamente después de la instalación, pero debe configurar manualmente el recopilador de datos, que es un componente del agente, para supervisar las instancias de servidor de aplicaciones.

Antes de empezar

- Asegúrese de que se cumplen los requisitos de acceso del usuario en el entorno. Para obtener instrucciones, consulte "Comprobación de los requisitos de acceso de usuario" en la página 866.
- Si en el servidor de aplicaciones que se va a supervisar existen otros recopiladores de datos, realice las acciones adecuadas para evitar conflictos de recopilador de datos. Para obtener instrucciones, consulte "Manejo de otros recopiladores de datos existentes en el servidor de aplicaciones" en la página 866.

Acerca de esta tarea

Importante:

- Si desea configurar el recopilador de datos sólo para la supervisión de recursos o establecer opciones adicionales, utilice el procedimiento de configuración completa. Para obtener instrucciones, consulte "Configuración o reconfiguración del recopilador de datos con los programas de utilidad de configuración completa" en la página 869.
- Si desea cambiar el nombre del servidor en la interfaz de usuario de supervisión, reconfigure el recopilador de datos y especifique un alias de servidor. Para obtener instrucciones, consulte "Configuración o reconfiguración del recopilador de datos con los programas de utilidad de configuración completa" en la página 869.

Para el Agente de WebSphere Applications, las variables *dir_inicio_dc* hacen referencia al directorio de inicio del recopilador de datos. La ubicación de la variable *dir_inicio_dc* en cada sistema operativo es la siguiente:

- Windows *dir_instal*\dchome\7.3.0.14.08
- Linux AIX *dir_instal*/yndchome/7.3.0.14.08

Procedimiento

1. Inicie la sesión en el sistema con el ID de usuario utilizado para instalar el servidor de aplicaciones.
2. Cambie al directorio `bin` del directorio de inicio del recopilador de datos.
   - Windows *dir_instalación*\dchome\7.3.0.14.08\bin
   - Linux AIX *dir_instalación*/yndchome/7.3.0.14.08/bin
3. Ejecute el siguiente programa de utilidad de configuración simple:
   - Windows `simpleconfig.bat`
   - Linux AIX `./simpleconfig.sh`

   El programa de utilidad **simpleconfig** descubre automáticamente los directorios de inicio de los servidores de aplicaciones.
4. Siga las solicitudes para continuar con la configuración del recopilador de datos.

   Será necesario que realice las siguientes acciones, en función de los valores del servidor de aplicaciones:
   - Para WebSphere Application Server tradicional:
     - Seleccione el directorio de instalación de WebSphere descubierto automáticamente o especifique manualmente el directorio de instalación.
     - Seleccione el perfil de WebSphere Application Server para supervisar.
     - Seleccione el perfil de propiedades de seguridad que debe utilizarse o proporcione el nombre de usuario y la contraseña de la consola de administración de WebSphere (si la seguridad está habilitada para el servidor de aplicaciones).
   - Para WebSphere Application Server Liberty:
     - Especifique la vía de acceso completa del directorio inicial de Liberty que contiene los directorios `bin` y `servers` (por ejemplo, `/opt/ibm/wlp`).
     - Especifique el directorio inicial del JRE utilizado por Liberty.
5. Si es posible, reinicie la instancia del servidor de aplicaciones una vez finalizada la configuración del recopilador de datos.
   a) Vaya al directorio `bin` bajo el directorio de inicio del perfil de servidor de aplicaciones. Por ejemplo, `opt/IBM/WebSphere/AppServer/profiles/`*nombre_perfil*`/bin`.
   b) Detenga el servidor de aplicaciones especificando el mandato **stopServer** en la consola de mandatos.
      - Linux AIX `./stopServer.sh` *nombre_servidor*
      - Windows `stopServer.bat` *nombre_servidor*
   c) Cuando se le solicite, especifique el ID de usuario y la contraseña del administrador de la consola de administración de WebSphere.
   d) Inicie de nuevo el servidor de aplicaciones especificando el mandato **startServer** en la consola de mandatos.
      - Linux AIX `./startServer.sh` *nombre_servidor*
      - Windows `startServer.bat` *nombre_servidor*

Resultados

- El recopilador de datos se configura para supervisar todas las instancias de un perfil, o bien, para WebSphere Application Server Liberty, una única instancia o varias instancias en el mismo directorio. Para supervisar más perfiles e instancias, repita la configuración.
- El recopilador de datos se ha configurado en las instancias del servidor, proporcionando una máxima supervisión.

- Para Cloud APM, Base, se ha habilitado la supervisión de recursos.
- Para Cloud APM, Advanced, se han habilitado la supervisión de recursos, el rastreo de transacciones y los datos de diagnóstico.

Limitación conocida: Al supervisar WebSphere Application Server Liberty, el recopilador de datos no puede generar sucesos JNDI (Java Naming and Directory Interface).

Qué hacer a continuación

- Inicie la sesión en la Consola de Cloud APM y utilice el editor de aplicaciones para añadir el servidor de aplicaciones supervisado al Panel de instrumentos del rendimiento de aplicaciones. Si desea instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte "Gestión de aplicaciones" en la página 1133.

  Recuerde: si el Agente de WebSphere Applications está configurado para supervisar WebSphere Portal Server, el agente está relacionado con el componente de aplicación de WebSphere Portal Server en el Panel de instrumentos del rendimiento de aplicaciones, no con WebSphere Application Server.
- Si la interfaz del usuario de supervisión en la Panel de instrumentos del rendimiento de aplicaciones no muestra información de la instancia del servidor de aplicaciones, reinicie el componente del agente de supervisión del Agente de WebSphere Applications completando los pasos siguientes:
  - Windows

    ```
    cd dir_instalación\bin
    was-agent.bat stop
    was-agent.bat start
    ```
  - Linux AIX

    ```
    cd dir_instalación/bin
    ./was-agent.sh
    stop
    ./was-agent.sh start
    ```

Configuración o reconfiguración del recopilador de datos con los programas de utilidad de configuración completa

Para establecer opciones de configuración adicionales, puede utilizar los programas de utilidad de configuración completa (interactivos o silenciosos) para configurar el recopilador de datos en lugar del programa de utilidad de configuración simple. También puede utilizar programas de utilidad de configuración completa para reconfigurar el recopilador de datos cuando ya esté configurado. Además, debe utilizar el programa de utilidad de configuración completa para configurar la supervisión de instancias de WebSphere Portal Server.

Antes de empezar

- Asegúrese de que se cumplen los requisitos de acceso del usuario en el entorno. Para obtener instrucciones, consulte "Comprobación de los requisitos de acceso de usuario" en la página 866.
- Si en el servidor de aplicaciones que se va a supervisar existen otros recopiladores de datos, realice las acciones adecuadas para evitar conflictos de recopilador de datos. Para obtener instrucciones, consulte "Manejo de otros recopiladores de datos existentes en el servidor de aplicaciones" en la página 866.

Acerca de esta tarea

Los programas de utilidad de configuración y reconfiguración pueden encontrarse en los directorios siguientes:

- Windows *dir_instalación*\dchome\7.3.0.14.08\bin
- Linux AIX *dir_instalación*/yndchome/7.3.0.14.08/bin

Procedimiento

- El programa de utilidad de configuración se denomina **config**. Es posible que necesite configurar el recopilador de datos con el programa de utilidad de configuración completa en los casos siguientes:
  - El programa de utilidad de configuración **simpleconfig** falla.
  - Desea configurar la supervisión de instancias de WebSphere Portal Server.
  - Desea especificar un alias de servidor que se visualiza en la interfaz de usuario de supervisión durante la configuración del recopilador de datos.
  - Desea tener más control sobre qué datos deben recopilarse. Por ejemplo, desea utilizar sólo la supervisión de recursos e inhabilitar los datos de diagnóstico y el rastreo de transacciones.
  - No desea configurar todos los servidores de aplicaciones dentro del mismo perfil simultáneamente.
  - El recopilador de datos no está configurado en el servidor de aplicaciones y desea volver a configurarlo.

  Para obtener información sobre el programa de utilidad de configuración completa interactivo, consulte "Configuración interactiva del recopilador de datos" en la página 870.
- El programa de utilidad de reconfiguración se denomina **reconfig**. Es posible que deba volver a configurar el recopilador de datos en los casos siguientes:
  - Desea reconfigurar el recopilador de datos después de que se haya configurado de forma interactiva o silenciosa.

  Para obtener información sobre el programa de utilidad de reconfiguración interactivo, consulte "Reconfiguración interactiva del recopilador de datos" en la página 875.
- Para la configuración silenciosa, consulte "Configuración del recopilador de datos en modalidad silenciosa" en la página 878.

Configuración interactiva del recopilador de datos

Utilice el programa de utilidad de configuración interactiva (`config.sh` o `config.bat`) para configurar el recopilador de datos cuando falle el programa de utilidad `simpleconfig`. Puede utilizar el programa de utilidad `config.sh` o `config.bat` para configurar el recopilador de datos para cada instancia de servidor de aplicaciones que desee supervisar.

Antes de empezar

Si va a configurar el recopilador de datos para supervisar WebSphere Application Server Liberty, establezca la variable de entorno de sistema **JAVA_HOME** en la misma JVM que la utilizada para el servidor de aplicaciones. Por ejemplo, en un sistema Windows, establezca el valor de **JAVA_HOME** en `C:\Archivos de programa\IBM\java`. O bien, en un sistema Linux, ejecute `export JAVA_HOME=/opt/IBM/java`.

Acerca de esta tarea

Utilice el siguiente programa de utilidad de configuración completa para configurar el recopilador de datos:

- Windows *dir_instalación*`\dchome\7.3.0.14.08\bin\config.bat`
- Linux AIX *dir_instalación*`/yndchome/7.3.0.14.08/bin/config.sh`

Procedimiento

Para configurar el recopilador de datos respondiendo a solicitudes, siga estos pasos:

1. Inicie la sesión en el sistema con el ID de usuario utilizado para instalar el servidor de aplicaciones.
2. Vaya al directorio `bin` del directorio de inicio del recopilador de datos *dc_home*.
3. Inicie el programa de utilidad de configuración emitiendo el siguiente mandato:
   - Windows `config.bat`

- Linux AIX `./config.sh`

  El programa de utilidad de configuración muestra las direcciones IP y nombres de host de todas las tarjetas de red que se encuentran en el sistema local.

4. Especifique el número que corresponda a la dirección IP y nombre de host. Si la dirección IP y el nombre de host que desea utilizar no están en la lista, especifique la dirección IP o el nombre de host.
5. Especifique el directorio de inicio del servidor de aplicaciones que se va a supervisar.
   - Para WebSphere Application Server tradicional, especifique el número que corresponde a un directorio de inicio de un servidor de aplicaciones descubierto automáticamente o especifique una vía de acceso completa a un directorio de inicio de servidor de aplicaciones.
   - Para WebSphere Application Server Liberty, especifique la vía de acceso completa al directorio de inicio de WebSphere Application Server Liberty que contiene los directorios `bin` y `servers`, por ejemplo `/opt/ibm/wlp`.
6. Si está configurando el recopilador de datos para WebSphere Application Server Liberty, se le solicitará el directorio de inicio de Java. Especifique el directorio de inicio de Java que se utiliza para el servidor de aplicaciones. Por ejemplo, `/opt/IBM/java`.
7. Cuando el programa de utilidad de configuración liste todos los perfiles bajo el directorio de inicio del servidor de aplicaciones especificado, especifique el número correspondiente al perfil del servidor de aplicaciones que desee configurar.
   - Para WebSphere Application Server tradicional, el programa de utilidad de configuración indica si WebSphere Global Security está habilitada para el perfil de WebSphere Application Server que ha especificado. Si la seguridad global no está habilitada, vaya al paso “9” en la página 871.
   - Para WebSphere Application Server Liberty, vaya al paso “10” en la página 871.
8. Si la seguridad global está habilitada para el perfil de WebSphere Application Server, especifique si se deben recuperar los valores de seguridad de un archivo de propiedades del cliente. Especifique 1 para permitir que el programa de utilidad de configuración recupere el nombre de usuario y la contraseña del archivo de propiedades de cliente correspondiente. En caso contrario, especifique 2 para indicar el nombre de usuario y la contraseña.

   El recopilador de datos se comunica con los Servicios administrativos de WebSphere utilizando invocación a método remoto (RMI) o el protocolo SOAP. Si la seguridad global está habilitada para un perfil, debe especificar el ID de usuario y la contraseña de un usuario que tenga autorización para iniciar sesión en la consola administrativa de WebSphere Application Server para el perfil del servidor de aplicaciones. O bien puede cifrar el nombre de usuario y la contraseña y almacenarlos en archivos de propiedades de cliente antes de configurar el recopilador de datos. Debe utilizar el archivo `sas.client.props` para una conexión RMI o el archivo `soap.client.props` para una conexión SOAP.
9. Cuando se le solicite el nombre de host de la consola de administración de WebSphere, pulse Intro para aceptar el valor predeterminado o especifique el nombre de host o la dirección IP de la consola de administración de WebSphere. El valor predeterminado es `localhost`.

   Recuerde: Para un entorno de despliegue de red, escriba el nombre de host o la dirección IP del gestor de despliegue.
10. Cuando el programa de utilidad de configuración muestre todas las instancias de servidor que todavía no están configuradas para la recopilación de datos, seleccione una o varias instancias de servidor de aplicaciones de la lista. Especifique el número correspondiente a la instancia de servidor de aplicaciones para configurar la recopilación de datos o especifique un asterisco (`*`) para configurar todas las instancias de servidor de aplicaciones para la recopilación de datos. Para especificar un subconjunto de servidores, especifique los números, separados por comas, que representan los servidores.
    Por ejemplo, `1,2,3`.

    Recuerde:

- Para un entorno autónomo, las instancias de servidor de aplicaciones deben estar ejecutándose durante la configuración. (No es necesario que una instancia de WebSphere Application Server Liberty esté en ejecución).
- En un entorno de Network Deployment, el gestor de despliegue debe estar en ejecución.
- Asegúrese de que las instancias de servidor de aplicaciones que seleccione son los servidores reales que alojan las aplicaciones o los servicios que desea supervisar.

11. En la sección **Integración con Agente para aplicaciones WebSphere**, especifique que desea integrar el recopilador de datos con el Agente de WebSphere Applications. Debe especificar 1 para seleccionar esta opción de integración y, a continuación, pulse Intro.

    El servidor seleccionado se registrará para la supervisión de recursos PMI.
12. si está configurando el recopilador de datos para WebSphere Application Server tradicional, especifique si desea configurar el recopilador de datos dentro de la instancia del servidor de aplicaciones.
    - Especifique 1 para configurar el recopilador de datos en el servidor de aplicaciones. Con esta opción, el recopilador de datos se integra con el servidor de aplicaciones, lo cual es necesario para utilizar la gama completa de supervisión de operaciones y recopilación de datos de diagnóstico. No obstante, la configuración del recopilador de datos en el servidor de aplicaciones requiere reiniciar el servidor de aplicaciones. Además, el recopilador de datos puede afectar al rendimiento del servidor.
    - Especifique 2 para no configurar el recopilador de datos en el servidor de aplicaciones y continúe en el paso “14” en la página 872. Con esta opción, el recopilador de datos se ejecuta como proceso autónomo y sólo puede habilitarse la supervisión de recursos.
13. Cuando se le solicite, especifique si se debe habilitar el recopilador de datos para los datos de diagnóstico. Especifique 1 para habilitar la recopilación de datos de diagnóstico. El valor predeterminado es 2.
14. Cuando se le solicite el nombre de host del agente de supervisión V8, especifique el nombre de host o la dirección IP del Agente de WebSphere Applications o pulse Intro para aceptar el valor predeterminado. El valor predeterminado corresponde a su opción en el paso 3.

    El agente de supervisión V8 hace referencia al Agente de WebSphere Applications, que se instala con IBM Cloud Application Performance Management.
15. Cuando se le solicite el número de puerto del agente de supervisión V8, especifique el número de puerto del Agente de WebSphere Applications o pulse Intro para aceptar el valor predeterminado. El valor predeterminado es 63335.
16. Cuando se le solicite si desea configurar el agente de supervisión V6 para aplicaciones WebSphere, pulse Intro para aceptar el valor predeterminado No.

    El agente de supervisión V6 hace referencia al ITCAM Agent for WebSphere Applications, que se instala en la antigua infraestructura de IBM® Tivoli® Monitoring. La configuración del agente de supervisión V6 sólo es necesaria para el entorno de coexistencia de agentes.
17. Cuando se le solicite el alias de servidor, pulse Intro para aceptar el valor predeterminado o especifique otro alias. Si está configurando varias instancias de servidor de aplicaciones, el programa de utilidad de configuración le solicitará un alias para cada instancia.

    Importante: El alias puede contener solo los caracteres siguientes: A-Z, a-z, subrayado (_), guión (-) y punto (.). No utilice otros caracteres en el alias.

    El alias de servidor es el primer calificador del nombre de instancia de agente (conocido también como MSN) que se visualiza en la Consola de Cloud APM. El valor predeterminado es el nombre del nodo combinado con el nombre del servidor. Por ejemplo, el alias **node1server1** indica el servidor denominado **server1** en el nodo denominado **node1**.
18. Cuando se le solicite un número de puerto para la supervisión de recursos PMI, pulse Intro para aceptar el valor predeterminado o especifique un número nuevo. El puerto predeterminado es 63355.

Este puerto se utiliza para la comunicación interna entre los componentes que se ejecutan en el mismo host. Si el puerto predeterminado está en uso, puede establecer un número diferente.

19. En la sección **Soporte para el rastreo de transacciones**, especifique si debe habilitarse el rastreo de transacciones. Especifique 1 para habilitar el soporte para el rastreo de transacciones. De lo contrario, especifique 2 y vaya al paso "22" en la página 873.
20. Cuando se le solicite el nombre de host o la dirección IP de la extensión de infraestructura de transacciones (Transaction Framework Extension), pulse Intro para aceptar el valor predeterminado o especifique otro nombre de host o dirección IP.

    La extensión de infraestructura de transacciones es un componente interno del Agente de WebSphere Applications que recopila métricas desde el recopilador de datos.
21. Cuando se le solicite el número de puerto que el recopilador de datos utiliza para conectarse a la extensión de infraestructura de transacciones, pulse Intro para aceptar el valor predeterminado o especifique otro número de puerto. El valor predeterminado es 5457.
22. Especifique si se debe integrar el recopilador de datos con Application Performance Diagnostics Lite. Pulse Intro para aceptar el valor predeterminado, No.
23. En la sección **Configuración avanzada**, especifique si desea cambiar la vía de acceso de registro de recogida de basura. Especifique 1 para seleccionar una vía de acceso del registro de recogida de basura. De lo contrario, especifique 2 y vaya al paso "25" en la página 873. Para utilizar la vía de acceso de registro que ya se ha especificado en el argumento de JVM del servidor de aplicaciones, especifique 2.
24. Especifique la vía de acceso de registro de recogida de basura. Especifique un nombre de archivo con su vía de acceso completa. Para WebSphere Application Server Liberty, no utilice variables en la vía de acceso. El recopilador de datos modifica automáticamente el nombre de archivo de registro, añadiéndole la información de instancia de servidor.

    Por ejemplo, si especifica `gc.log` como nombre de archivo, el nombre real se establece en *`nombre_perfil.nombre_célula.nombre_nodo.nombre_servidor`*`.gc.log` para cada instancia de servidor de aplicaciones configurada.

    Importante: En la vía de acceso del registro de recogida de basura, puede utilizar variables de WebSphere como por ejemplo `${SERVER_LOG_ROOT}`. No obstante, no utilice plantillas, como `%pid`.
25. Revise el resumen de la configuración del recopilador de datos que se aplicará a las instancias de servidor de aplicaciones especificadas. Si es necesario, vuelva a configurar las partes de la configuración del recopilador de datos antes de aplicar los cambios.
26. Especifique a para aceptar los cambios.
27. Cuando se le solicite, especifique si desea crear una copia de seguridad de la configuración actual. Especifique 1 para crear una copia de seguridad de la configuración actual. De lo contrario, especifique 2.

    El programa de utilidad de configuración aplica los cambios y presenta un mensaje de estado para indicar que la configuración del recopilador de datos para el perfil se ha completado.
28. Si está configurando el recopilador de datos para WebSphere Application Server tradicional, reinicie las instancias del servidor de aplicaciones o reinicie el agente, en función de su elección en el paso "12" en la página 872.
    - Si ha habilitado el recopilador de datos en el servidor de aplicaciones, reinicie las instancias de servidor de aplicaciones tal como se indica en el programa de utilidad de configuración.
    - Si ha habilitado la supervisión de recursos de PMI sin habilitar el recopilador de datos en el servidor de aplicaciones, reinicie el Agente de WebSphere Applications ejecutando los mandatos siguientes:
      – Windows

      ```
      cd dir_instalación\bin
      was-agent.bat stop
      was-agent.bat start
      ```

– Linux AIX

```
cd dir_instalación/bin
./was-agent.sh
stop
./was-agent.sh start
```

La configuración del recopilador de datos entra en vigor una vez reiniciado el servidor de aplicaciones o el agente.

29. Inicie la sesión en Consola de Cloud APM para ver los datos en los paneles de instrumentos.
    a) Acceda a la consola mediante el enlace que se proporciona en el correo electrónico que le informa de que el servicio está preparado. También puede acceder a la consola desde el sitio web IBM Marketplace. Para obtener instrucciones detalladas, consulte "Inicio de la Consola de Cloud APM" en la página 1009.
    b) Utilice el editor de aplicaciones para añadir el servidor de aplicaciones supervisado al Panel de instrumentos del rendimiento de aplicaciones. Puede añadirlo como componente nuevo a la aplicación existente o crear una aplicación para que contenga este componente.

    Para obtener más información sobre el editor de aplicaciones, consulte "Gestión de aplicaciones" en la página 1133.

Qué hacer a continuación

- Si el ID de usuario actual utilizado para configurar el recopilador de datos no es el mismo ID del usuario que ejecuta el servidor de aplicaciones, compruebe que el ID de usuario para configurar el recopilador de datos tenga permisos de lectura y escritura sobre los directorios `runtime` y `logs` del directorio de inicio del recopilador de datos. Estos dos subdirectorios los crea el ID del usuario que ejecuta el servidor de aplicaciones cuando éste se reinicia.
- Inicie la sesión en Consola de Cloud APM para ver los datos de supervisión en los paneles de instrumentos. Si los datos de supervisión no están disponibles de inmediato, reinicie el Agente de WebSphere Applications ejecutando los mandatos siguientes:
  – Windows

  ```
  cd dir_instalación\bin
  was-agent.bat stop
  was-agent.bat start
  ```

  – Linux AIX

  ```
  cd dir_instalación/bin
  ./was-agent.sh
  stop
  ./was-agent.sh start
  ```

- Al cambiar el alias de servidor se cambia el nombre de la instancia de agente que se ha registrado con la Consola de Cloud APM. Si no es la primera vez que configura el recopilador de datos y ha cambiado el alias de servidor, debe borrar algunos archivos de la memoria caché siguiendo estos pasos:
  1. Detenga el agente de supervisión si se está ejecutando.
  2. Abra el archivo *nombre_host*`_yn.xml` en el directorio siguiente con un editor de texto, donde *nombre_host* es el nombre del host en el que el Agente de WebSphere Applications está instalado.
     – Windows *dir_instalación*`\TMAITM6_x64` (El valor predeterminado es `C:\IBM\APM\TMAITM6_x64`)
     – Linux AIX *dir_instalación*`/config` (El valor predeterminado es `/opt/ibm/apm/agent/config`)

3. Busque la línea que empieza con la serie siguiente y contiene el nombre de servidor anterior. Por ejemplo, `was85.win4net01Cell02.win4net01Node02.AppSrv01.server1`, donde `server1` es el nombre anterior del servidor de aplicaciones.

   ```
   <!ENTITY cód_producto_was.nombre_célula.nombre_nodo.nombre_perfil.nombre_servidor
   ```

   donde *cód_producto_was* es el código de producto de WebSphere Application Server; *nombre_célula* es el nombre de la célula; *nombre_nodo* es el nombre de nodo; *nombre_perfil* es el nombre de perfil del servidor de aplicaciones; *nombre_servidor* es el nombre anterior del servidor de aplicaciones.
4. Busque el archivo `.XML` que se indica en la línea dentro del directorio actual y suprima el archivo.
5. Elimine la línea que ha localizado en el paso 3 en el archivo *nombre_host*`_yn.xml`.
6. Al final del archivo *nombre_host*`_yn.xml`, elimine la línea que contiene los nombres de servidor anteriores.
7. Guarde los cambios y cierre el archivo.
8. Reinicie el agente de supervisión.

Reconfiguración interactiva del recopilador de datos

Si ha configurado el recopilador de datos para supervisar una o más instancias de servidor de aplicaciones, puede volver a configurarlo utilizando el programa de utilidad de reconfiguración (`reconfig.sh` o `reconfig.bat`).

Antes de empezar

Si va a configurar el recopilador de datos para supervisar WebSphere Application Server Liberty, establezca la variable de entorno de sistema **JAVA_HOME** en la misma JVM que la utilizada para el servidor de aplicaciones. Por ejemplo, en un sistema Windows, establezca el valor de **JAVA_HOME** en `C:\Archivos de programa\IBM\java`. O bien, en un sistema Linux, ejecute `export JAVA_HOME=/opt/IBM/java`.

Acerca de esta tarea

Utilice el siguiente programa de utilidad de reconfiguración completa para configurar el recopilador de datos:

- Windows *dir_instalación*`\dchome\7.3.0.14.08\bin\reconfig.bat`
- Linux AIX *dir_instalación*`/yndchome/7.3.0.14.08/bin/reconfig.sh`

Recuerde: el programa de utilidad **reconfig** no es aplicable en los casos siguientes. Utilice el programa de utilidad de configuración **config** en su lugar. Aunque el programa de utilidad **config** advierte que el servidor ya está configurado, puede realizar los cambios necesarios.

- El recopilador de datos ya está configurado sólo para la supervisión de recursos y desea reconfigurarlo.
- Desea reconfigurar el recopilador de datos para WebSphere Portal Server.

Consejo: en los indicadores que le solicitan los valores de configuración del agente, el programa de utilidad de reconfiguración ofrece los valores configurados actualmente como valores predeterminados.

Procedimiento

Para reconfigurar el recopilador de datos respondiendo a solicitudes, siga estos pasos:

1. Inicie la sesión en el sistema con el ID de usuario utilizado para instalar el servidor de aplicaciones.
2. Vaya al directorio `bin` del directorio de inicio del recopilador de datos *dc_home*.
3. Inicie el programa de utilidad de reconfiguración emitiendo el siguiente mandato:
   - Windows `reconfig.bat`
   - Linux AIX `./reconfig.sh`

Consejo: La ejecución de este programa de utilidad de reconfiguración tiene el mismo efecto que ejecutar el script `config.bat` con el argumento `-reconfig` en sistemas Windows o el script `config.sh` con el argumento `-reconfig` en sistemas Linux o AIX.

El programa de utilidad de reconfiguración muestra las direcciones IP de todas las tarjetas de red que se encuentran en el sistema local.

4. Especifique el número que corresponda a la dirección IP que se va a utilizar.

   El programa de utilidad de reconfiguración visualiza todas las instancias de servidor de aplicaciones para las que está configurado el recopilador de datos en este host y le solicita que seleccione una o varias instancias de servidor de aplicaciones de la lista.
5. Seleccione una o más instancias de servidor de aplicaciones de la lista. Especifique el número que corresponde a la instancia de servidor de aplicaciones para la que se debe volver a configurar la recopilación de datos o especifique un asterisco (*) para volver a configurar todas las instancias de servidor de aplicaciones para la recopilación de datos. Para especificar un subconjunto de servidores, especifique los números, separados por comas, que representan los servidores. Por ejemplo: `1,2,3`.

   Recuerde:

   - Para un entorno autónomo, las instancias de servidor de aplicaciones deben estar ejecutándose durante la configuración. (No es necesario que una instancia de WebSphere Application Server Liberty esté en ejecución).
   - En un entorno de Network Deployment, el gestor de despliegue debe estar en ejecución.
   - Asegúrese de que las instancias de servidor de aplicaciones que seleccione son los servidores reales que alojan las aplicaciones o los servicios que desea supervisar.
6. En la sección **Integración con Agente para aplicaciones WebSphere**, especifique que desea integrar el recopilador de datos con el Agente de WebSphere Applications. Debe especificar 1 para seleccionar esta opción de integración y, a continuación, pulse Intro.
7. si está configurando el recopilador de datos para WebSphere Application Server tradicional, especifique si desea configurar el recopilador de datos dentro de la instancia del servidor de aplicaciones.

   - Especifique 1 para configurar el recopilador de datos en el servidor de aplicaciones. Con esta opción, el recopilador de datos se integra con el servidor de aplicaciones, lo cual es necesario para utilizar la gama completa de supervisión de operaciones y recopilación de datos de diagnóstico. No obstante, la configuración del recopilador de datos en el servidor de aplicaciones requiere reiniciar el servidor de aplicaciones. Además, el recopilador de datos puede afectar al rendimiento del servidor.
   - Especifique 2 para no configurar el recopilador de datos en el servidor de aplicaciones y continúe en el paso “9” en la página 876. Con esta opción, el recopilador de datos se ejecuta como proceso autónomo y sólo puede habilitarse la supervisión de recursos de PMI.
8. Cuando se le solicite, especifique si desea habilitar la recopilación de datos de diagnóstico para el recopilador de datos. Escriba 1 para sí o 2 para no.
9. Cuando se le solicite el nombre de host, especifique el nombre de host o la dirección IP del Agente de WebSphere Applications o pulse Intro para aceptar el valor predeterminado. El valor predeterminado corresponde a su elección en el paso “4” en la página 876.
10. Cuando se le solicite el número de puerto, especifique el número de puerto del agente de supervisión o pulse Intro para aceptar el valor predeterminado. El valor predeterminado es 63335.
11. Cuando se le solicite si desea configurar el agente de supervisión V6 para aplicaciones WebSphere, pulse Intro para aceptar el valor predeterminado No.

    El agente de supervisión V6 hace referencia al ITCAM Agent for WebSphere Applications, que se instala en la antigua infraestructura de IBM® Tivoli® Monitoring. La configuración del agente de supervisión V6 sólo es necesaria para el entorno de coexistencia de agentes.
12. Cuando se le solicite el alias de servidor, pulse Intro para aceptar el valor predeterminado o especifique otro alias. Si está configurando varias instancias de servidor de aplicaciones, el programa de utilidad de configuración le solicitará un alias para cada instancia.

Importante: El alias puede contener solo los caracteres siguientes: A-Z, a-z, subrayado (_), guión (-) y punto (.). No utilice otros caracteres en el alias.

El alias de servidor es el primer calificador del nombre de instancia de agente (conocido también como MSN) que se visualiza en la Consola de Cloud APM. El valor predeterminado es el nombre del nodo combinado con el nombre del servidor. Por ejemplo, el alias **node1server1** indica el servidor denominado **server1** en el nodo denominado **node1**.

13. Cuando se le solicite un número de puerto para la supervisión de recursos PMI, pulse Intro para aceptar el valor predeterminado o especifique un número nuevo. El puerto predeterminado es 63355.

    Este puerto se utiliza para la comunicación interna entre los componentes que se ejecutan en el mismo host. Si el puerto predeterminado está en uso, puede establecer un número diferente.
14. En la sección **Soporte para el rastreo de transacciones**, especifique si debe habilitarse el rastreo de transacciones. Especifique 1 para habilitar el soporte para el rastreo de transacciones. De lo contrario, especifique 2 y vaya al paso "17" en la página 877.
15. Cuando se le solicite el nombre de host o la dirección IP de la extensión de infraestructura de transacciones (Transaction Framework Extension), pulse Intro para aceptar el valor predeterminado o especifique otro nombre de host o dirección IP.

    La extensión de infraestructura de transacciones es un componente interno del Agente de WebSphere Applications que recopila métricas desde el recopilador de datos.
16. Cuando se le solicite el número de puerto que el recopilador de datos utiliza para conectarse a la extensión de infraestructura de transacciones, pulse Intro para aceptar el valor predeterminado o especifique otro número de puerto. El valor predeterminado es 5457.
17. Especifique si se debe integrar el recopilador de datos con Application Performance Diagnostics Lite. Pulse Intro para aceptar el valor predeterminado No.
18. En la sección **Configuración avanzada**, especifique si desea cambiar la vía de acceso de registro de recogida de basura.

    Especifique 1 para seleccionar una vía de acceso del registro de recogida de basura. De lo contrario, especifique 2 y vaya al paso "20" en la página 877. Para utilizar la vía de acceso de registro que ya se ha especificado en el argumento de JVM del servidor de aplicaciones, especifique 2.
19. Especifique la vía de acceso de registro de recogida de basura. Especifique un nombre de archivo con su vía de acceso completa. Para WebSphere Application Server Liberty, no utilice variables en la vía de acceso. El recopilador de datos modifica automáticamente el nombre de archivo de registro, añadiéndole la información de instancia de servidor.

    Por ejemplo, si especifica `gc.log` como nombre de archivo, el nombre real se establece en *`nombre_perfil.nombre_célula.nombre_nodo.nombre_servidor`*`.gc.log` para cada instancia de servidor de aplicaciones configurada.

    Importante: En la vía de acceso del registro de recogida de basura, puede utilizar variables de WebSphere como por ejemplo `${SERVER_LOG_ROOT}`. No obstante, no utilice plantillas, como `%pid`.
20. Revise el resumen de la configuración del recopilador de datos que se aplicará a las instancias de servidor de aplicaciones especificadas. Vuelva a configurar las partes de la configuración del recopilador de datos antes de aplicar los cambios, si es necesario.
21. Especifique a para aceptar los cambios.
22. Cuando se le solicite, especifique si desea crear una copia de seguridad de la configuración actual. Especifique 1 para crear una copia de seguridad de la configuración actual. De lo contrario, especifique 2.

    El programa de utilidad de configuración aplica los cambios y presenta un mensaje de estado para indicar que la configuración del recopilador de datos para el perfil se ha completado.
23. Si está configurando el recopilador de datos para WebSphere Application Server tradicional, reinicie las instancias del servidor de aplicaciones o reinicie el agente, en función de su elección en el paso "7" en la página 876.

- Si ha habilitado el recopilador de datos en el servidor de aplicaciones, reinicie las instancias de servidor de aplicaciones tal como se indica en el programa de utilidad de configuración.
- Si ha habilitado la supervisión de recursos de PMI sin habilitar el recopilador de datos en el servidor de aplicaciones, reinicie el Agente de WebSphere Applications ejecutando los mandatos siguientes:
  - Windows

    ```
    cd dir_instalación\bin
    was-agent.bat stop
    was-agent.bat start
    ```

  - Linux AIX

    ```
    cd dir_instalación/bin
    ./was-agent.sh
    stop
    ./was-agent.sh start
    ```

  La configuración del recopilador de datos entra en vigor una vez reiniciado el servidor de aplicaciones o el agente.

Qué hacer a continuación

- Al cambiar el alias de servidor se cambia el nombre de la instancia de agente que se ha registrado con la Consola de Cloud APM. Si ha cambiado el alias de servidor durante el procedimiento de reconfiguración, debe borrar algunos archivos de la memoria caché siguiendo estos pasos:
  1. Detenga el agente de supervisión si se está ejecutando.
  2. Abra el archivo *nombre_host*_yn.xml en el directorio siguiente con un editor de texto, donde *nombre_host* es el nombre del host en el que el Agente de WebSphere Applications está instalado.
     - Windows *dir_instalación*\TMAITM6_x64 (El valor predeterminado es C:\IBM\APM\TMAITM6_x64)
     - Linux AIX *dir_instalación*/config (El valor predeterminado es /opt/ibm/apm/agent/config)
  3. Busque la línea que empieza con la serie siguiente y contiene el nombre de servidor anterior. Por ejemplo, was85.win4net01Cell02.win4net01Node02.AppSrv01.server1, donde server1 es el nombre anterior del servidor de aplicaciones.

     ```
     <!ENTITY cód_producto_was.nombre_célula.nombre_nodo.nombre_perfil.nombre_servidor
     ```

     donde *cód_producto_was* es el código de producto de WebSphere Application Server; *nombre_célula* es el nombre de la célula; *nombre_nodo* es el nombre de nodo; *nombre_perfil* es el nombre de perfil del servidor de aplicaciones; *nombre_servidor* es el nombre anterior del servidor de aplicaciones.
  4. Busque el archivo .XML que se indica en la línea dentro del directorio actual y suprima el archivo.
  5. Elimine la línea que ha localizado en el paso 3 en el archivo *nombre_host*_yn.xml.
  6. Al final del archivo *nombre_host*_yn.xml, elimine la línea que contiene los nombres de servidor anteriores.
  7. Guarde los cambios y cierre el archivo.
  8. Reinicie el agente de supervisión.

Configuración del recopilador de datos en modalidad silenciosa

Si desea configurar muchas instancias de servidor de aplicaciones, podría ser más conveniente configurar el recopilador de datos en modalidad silenciosa.

Acerca de esta tarea

Al configurar el recopilador de datos en modalidad silenciosa primero se deben especificar las opciones de configuración en un archivo de propiedades. Con el programa de utilidad de configuración se suministra un archivo de propiedades de ejemplo, `sample_silent_config.txt`. El archivo está disponible en los directorios siguientes, donde *dir_inicio_dc* es el directorio donde está instalado el recopilador de datos. Para la vía de acceso completa del directorio *dir_inicio_dc*, consulte la introducción en Configuración del recopilador de datos para el agente de aplicaciones WebSphere. .

- Windows *dir_inicio_dc*\bin
- Linux AIX *dir_inicio_dc*/bin

Si desea información detallada sobre cada propiedad de configuración disponible en este archivo, consulte "Archivo de propiedades para la configuración silenciosa del recopilador de datos" en la página 880.

Procedimiento

Siga estos pasos para realizar una configuración silenciosa:

1. Especifique las opciones de configuración en el archivo de propiedades. Puede copiar el archivo de propiedades de ejemplo y modificar las opciones necesarias.
2. Establezca la ubicación del directorio de inicio de Java antes de ejecutar el programa de utilidad. Por ejemplo:
   - Windows
     ```
     set JAVA_HOME=C:\Archivos de programa\IBM\WebSphere\AppServer80\java
     ```
   - Linux AIX
     ```
     export JAVA_HOME=/opt/IBM/AppServer80/java
     ```

   Importante: si está configurando la supervisión de WebSphere Application Server Liberty, debe utilizar la misma versión de JVM que se ha utilizado para el servidor de aplicaciones. De lo contrario, es posible que falle la supervisión.
3. Vaya al directorio siguiente:
   - Windows *dir_inicio_dc*\bin
   - Linux AIX *dir_inicio_dc*/bin
4. Ejecute el mandato para configurar el recopilador de datos en modalidad silenciosa.
   - Windows Ejecute el mandato siguiente como el administrador que ha instalado WebSphere Application Server.
     ```
     config.bat -silent [dir_vía_acceso]\archivo de instalación
     ```
   - Linux AIX Ejecute el siguiente mandato con privilegios de usuario root.
     ```
     config.sh -silent [vía_acceso_dir]/archivo silencioso
     ```

   Consejo: Si se ha utilizado el usuario `wsadmin` para instalar el servidor de aplicaciones, ejecute el programa de utilidad `config` con el usuario `wsadmin` o con privilegios de usuario root.
5. Tras configurar el recopilador de datos para supervisar instancias de servidor de aplicaciones, si ha habilitado el recopilador de datos en el servidor de aplicaciones debe reiniciar las instancias. La configuración del recopilador de datos se aplica cuando se reinician las instancias de servidor de aplicaciones.
6. Si ha habilitado la supervisión de recursos de PMI sin habilitar el recopilador de datos en el servidor de aplicaciones, puede que deba reiniciar el Agente de WebSphere Applications para iniciar la

supervisión. Si los datos de supervisión no están disponibles de inmediato, reinicie el agente de supervisión ejecutando los mandatos siguientes:

- Windows

```
cd dir_instalación\bin
was-agent.bat stop
was-agent.bat start
```

- Linux AIX

```
cd dir_instalación/bin
./was-agent.sh
stop
./was-agent.sh start
```

Qué hacer a continuación

Después de la configuración silenciosa, para reconfigurar el recopilador de datos, tiene dos opciones:

- Reconfigurarlo interactivamente mediante el programa de utilidad de reconfiguración **reconfig**. Para obtener instrucciones, consulte "Reconfiguración interactiva del recopilador de datos" en la página 875.
- Desconfigurarlo de forma silenciosa y, a continuación, utilizar el mismo procedimiento para volver a configurarlo de forma silenciosa. Si desea más instrucciones, consulte "Desconfiguración del recopilador de datos en modalidad silenciosa" en la página 156.

Referencia relacionada

"Archivo de propiedades para la configuración silenciosa del recopilador de datos" en la página 880
Para configurar de forma silenciosa el recopilador de datos, en primer lugar, especifique opciones de configuración en un archivo de propiedades y, a continuación, ejecute el programa de utilidad de la configuración.

Archivo de propiedades para la configuración silenciosa del recopilador de datos

Para configurar de forma silenciosa el recopilador de datos, en primer lugar, especifique opciones de configuración en un archivo de propiedades y, a continuación, ejecute el programa de utilidad de la configuración.

Al crear el archivo de propiedades, tenga en cuenta las siguientes consideraciones:

- Una línea en el archivo que empieza con un signo de número (#) se trata como un comentario y no se procesa. Si el signo de número se utiliza en cualquier otra posición de la línea, no se considera el inicio de un comentario.
- Cada propiedad se describe en una línea distinta, con el formato siguiente: *propiedad* = *valor*.

  propiedad
  Nombre de la propiedad. La lista de propiedades válidas que puede configurar se muestra en la Tabla 223 en la página 881.

  valor
  Valor de la propiedad. Ya se han proporcionado valores predeterminados para algunas propiedades. Puede suprimir los valores predeterminados para dejar los valores de propiedades en blanco o vacíos. Un valor vacío se trata como si la propiedad no se hubiera especificado, en vez de utilizar el valor predeterminado. Si desea utilizar valores predeterminados, marque como comentario la propiedad en el archivo.
- Las contraseñas están en texto sin formato.
- Las propiedades y los valores distinguen entre mayúsculas y minúsculas.

Tabla 223 en la página 881 describe las propiedades que están disponibles al configurar el recopilador de datos en modalidad silenciosa.

Importante: si está configurando el recopilador de datos para una instancia de WebSphere Application Server Liberty, algunas de las propiedades no se utilizan.

Tabla 223. Propiedades disponibles para la ejecución del programa de utilidad de configuración en modalidad silenciosa

Propiedad	Comentario
default.hostip	Si el sistema utiliza varias direcciones IP, especifique la dirección IP que debe utilizar el recopilador de datos.
Integración del recopilador de datos con el servidor de gestión ITCAM for Application Diagnostics **Importante:** El servidor de gestión sólo está disponible si tiene ITCAM for Application Diagnostics. Para una instancia de WebSphere Application Server Liberty o en un entorno Cloud APM, no se utilizan estas propiedades.	
ms.connect	Especifica si el recopilador de datos está configurado para conectarse al servidor de gestión en un entorno de ITCAM for Application Diagnostics. Los valores válidos son `True` y `False`.
ms.kernel.host	Especifica el nombre de host completo del servidor de gestión.
ms.kernel.codebase.port	Especifica el puerto codebase en el que escucha el servidor de gestión.
ms.am.home	Especifica el directorio de inicio del servidor de gestión.
ms.am.socket.bindip	Especifica la dirección IP o el nombre de host que el recopilador de datos debe utilizar para comunicarse con el servidor de gestión. Si hay más de una interfaz de red o dirección IP configurada en el sistema del recopilador de datos, elija una de ellas.
ms.probe.controller.rmi.port	Si el recopilador de datos está detrás de un cortafuegos o si tiene requisitos especiales para cambiar el puerto RMI de controlador del recopilador de datos, establezca este rango de números de puerto. Configure este número de puerto según lo permita el cortafuegos para cada host de recopilador de datos. Por ejemplo: `ms.probe.controller.rmi.port=8300-8399` o ms.probe.controller.rmi.port=8300.
ms.probe.rmi.port	Si el recopilador de datos se encuentra detrás de un cortafuegos, o si tiene requisitos especiales para cambiar el puerto RMI del recopilador de datos, establezca este rango de números de puerto. Configure este número de puerto según lo permita el cortafuegos para cada host de recopilador de datos. Por ejemplo: `ms.probe.rmi.port=8200-8299` o `ms.probe.rmi.port=8200`.
Soporte para el rastreo de transacciones Para ver la información de rastreo de transacciones, debe tener vistas de topología disponibles en la Consola de Cloud APM y habilitar el rastreo de transacciones en la ventana de configuración de agente.	
ttapi.enable	Especifica si el recopilador de datos da soporte de rastreo de transacciones. Los valores válidos son `True` y `False`.
ttapi.host	Especifica el host de la extensión de infraestructura de transacciones, que es el componente de Monitoring Agent for WebSphere Applications que recopila métricas del recopilador de datos. Utilice el valor de host local, `127.0.0.1`.
ttapi.port	Especifica el puerto de la extensión de infraestructura de transacciones. Utilice 5457.

Tabla 223. Propiedades disponibles para la ejecución del programa de utilidad de configuración en modalidad silenciosa (continuación)

Propiedad	Comentario
Integración del recopilador de datos con ITCAM for SOA **Importante:** Para una instancia de WebSphere Application Server Liberty o en un entorno Cloud APM, no se utiliza esta propiedad.	
soa.enable	Especifica si se debe integrar el recopilador de datos con ITCAM for SOA. Debe instalarse el agente ITCAM for SOA para completar la configuración.
Integración del recopilador de datos con Tivoli Performance Monitoring **Importante:** Para una instancia de WebSphere Application Server Liberty o en un entorno Cloud APM, no se utiliza esta propiedad.	
tpv.enable	Especifica si se debe integrar el recopilador de datos con Tivoli Performance Monitoring cuando el recopilador de datos se incluya como parte de ITCAM for WebSphere Application Server versión 8.5. Para acceder a Tivoli Performance Monitoring utilice la consola administrativa de WebSphere Application Server. Los valores válidos son *True* y *False*.
Integración del recopilador de datos con Application Performance Diagnostics Lite **Importante:** Para una instancia de WebSphere Application Server Liberty, esta propiedad no se utiliza.	
de.enable	Especifica si se deben recopilar datos de diagnóstico, necesarios para Application Performance Diagnostics y Application Performance Diagnostics Lite. Los valores válidos son `True` y `False`. Habilite esta integración si tiene Application Diagnostics o puede tenerlo en el futuro. En este caso, la recopilación de datos de diagnóstico se habilita al iniciarse el servidor. De lo contrario, se inhabilita al iniciar; puede habilitarla mediante la página Configuración de agente de la interfaz de usuario, pero si se reinicia el servidor, la recopilación de datos de diagnóstico se volverá a inhabilitar. Este valor habilita también la integración con Application Performance Diagnostics Lite, que es una herramienta para la investigación de diagnóstico de aplicaciones en ejecución en WebSphere Application Server y WebSphere Portal Server. Con esta herramienta, puede analizar datos en tiempo real o puede guardar información de diagnóstico en un archivo para su posterior análisis.
Supervisión del recopilador de datos y de recursos de PMI El servidor seleccionado está siempre configurado para la supervisión de recursos (PMI), sin cambios en el servidor de aplicaciones. Esta opción de supervisión proporciona métricas limitadas y funciona solo con el Agente de WebSphere Applications, pero no requiere reiniciar el servidor de aplicaciones ni puede afectar al rendimiento.	

Tabla 223. Propiedades disponibles para la ejecución del programa de utilidad de configuración en modalidad silenciosa (continuación)

Propiedad	Comentario
tema.appserver	Especifica si desea configurar el recopilador de datos dentro de la instancia de servidor de aplicaciones. El recopilador de datos dentro de la instancia de servidor de aplicaciones es necesario para todo el rango de métricas del Agente de WebSphere Applications y para la integración con cualquier otro producto. Sin embargo, la configuración del recopilador de datos requiere reiniciar el servidor de aplicaciones. Además, el recopilador de datos puede afectar al rendimiento del servidor. Los valores válidos son `True` y `False`. Si este parámetro se establece en `False`, los parámetros de configuración del recopilador de datos para la integración con productos que no sean Agente de WebSphere Applications se ignoran. Cuando este parámetro se establece en `False`, las funciones de diagnóstico y rastreo de transacciones no están disponibles, y sólo se recopilan datos de supervisión de recursos.
tema.jmxport	Número de puerto TCP/IP para la supervisión de recursos. El puerto se utiliza para la comunicación interna entre los componentes que se ejecutan en el mismo host. El puerto predeterminado es 63355; si este puerto está en uso, puede establecer otro número.
Integración del recopilador de datos con el componente de agente de supervisión de Agente de WebSphere Applications y con Application Performance Diagnostics Lite	
temaconnect	Especifica si el recopilador de datos se conecta al componente de agente de supervisión de Agente de WebSphere Applications. Los valores válidos son `True` y `False`. **Importante:** Debe utilizar el valor `True` para utilizar el Agente de WebSphere Applications.
tema.appserver	Especifica si desea configurar el recopilador de datos dentro de la instancia de servidor de aplicaciones. El recopilador de datos dentro de la instancia de servidor de aplicaciones es necesario para todo el rango de métricas del Agente de WebSphere Applications y para la integración con cualquier otro producto. Sin embargo, requiere reiniciar el servidor de aplicaciones. Además, el recopilador de datos puede afectar al rendimiento del servidor. Los valores válidos son `True` y `False`. Si este parámetro se establece en `False`, los parámetros de configuración para la integración del recopilador de datos con productos que no sean Agente de WebSphere Applications se omiten, así como los siguientes parámetros tema.host y tema.port. Cuando este parámetro se establece en `False`, las funciones de diagnóstico y rastreo de transacciones no están disponibles, y sólo se recopilan datos de supervisión de recursos.
tema.host	Especifica el nombre de host completo o la dirección IP del componente de agente de supervisión de Agente de WebSphere Applications. Utilice la dirección de host local (127.0.0.1).
tema.port	Especifica el número de puerto del componente de agente de supervisión de Agente de WebSphere Applications. No cambie el valor predeterminado de 63335.

Tabla 223. Propiedades disponibles para la ejecución del programa de utilidad de configuración en modalidad silenciosa (continuación)

Propiedad	Comentario
tema.jmxport	Número de puerto TCP/IP para la supervisión de recursos. El puerto se utiliza para la comunicación interna entre los componentes que se ejecutan en el mismo host. El puerto predeterminado es 63355; si este puerto está en uso, puede establecer otro número.
Integración del recopilador de datos con ITCAM Agent for WebSphere Applications versión 6 Utilice las propiedades siguientes para configurar un recopilador de datos para que recopile datos para Agente de WebSphere Applications y ITCAM Agent for WebSphere Applications versión 6.	
config.tema.v6	Especifica si se debe integrar el recopilador de datos con el componente de agente de supervisión de ITCAM Agent for WebSphere Applications versión 6. Los valores válidos son `True` y `False`. El valor predeterminado es `False`.
tema.host.v6	Especifica si se debe integrar el recopilador de datos con el componente de agente de supervisión de ITCAM Agent for WebSphere Applications versión 6. Los valores válidos son `True` y `False`. El valor predeterminado es `False`.
tema.port.v6	Especifica el número de puerto del componente de agente de supervisión de ITCAM Agent for WebSphere Applications versión 6. No cambie el valor predeterminado 63336.
Copia de seguridad de WebSphere Application Server	
was.backup.configuration	Especifica si se debe realizar una copia de seguridad de la configuración actual de WebSphere Application Server antes de aplicar la nueva configuración. Los valores válidos son `True` y `False`.
was.backup.configuration.dir	Especifica la ubicación del directorio de copia de seguridad.
Valores de configuración avanzada	
was.gc.custom.path	Especifica si se debe definir una vía de acceso personalizada para el registro de recogida de basura.
was.gc.file	Especifica la vía de acceso al registro de recogida de basura personalizada. Establezca este valor en un nombre de archivo con su vía de acceso completa. El recopilador de datos modifica automáticamente el nombre de archivo de registro, añadiéndole la información de instancia de servidor. Por ejemplo, si especifica `gc.log` como nombre de archivo, el nombre real se establece en *nombre_perfil*`.`*nombre_célula*`.`*nombre_nodo*`.`*nombre_servidor*`.gc.log` para cada instancia de servidor de aplicaciones configurada. **Importante:** En la vía de acceso al registro de recogida de basura, puede utilizar variables de WebSphere, como por ejemplo `${SERVER_LOG_ROOT}`. Sin embargo, no utilice plantillas, como %pid.
Valores de conexión de WebSphere Administrative Services	

Tabla 223. Propiedades disponibles para la ejecución del programa de utilidad de configuración en modalidad silenciosa (continuación)

Propiedad	Comentario
was.wsadmin.connection.host	Especifica el nombre del host al que se está conectando la herramienta wsadmin. En un entorno de Network Deployment, especifique la conexión wsadmin al gestor de despliegue. En un entorno autónomo, especifique la conexión wsadmin con el servidor. **Recuerde:** Si la consola administrativa de WebSphere está en el mismo sistema, se utilizará el valor de `localhost` para la conexión. Sin embargo, en algunos casos, `localhost` no está permitido para la comunicación debido a valores de seguridad o red del sistema. En este caso, debe especificar este parámetro en el archivo de respuestas silencioso.
was.wsadmin.connection.type	Especifica el puerto que la herramienta wsadmin debe utilizar para conectarse con WebSphere Application Server.
was.wsadmin.connection.port	Especifica el puerto que la herramienta wsadmin debe utilizar para conectarse con WebSphere Application Server.
Valores de seguridad global de WebSphere Application Server	
was.wsadmin.username	Especifica el ID de un usuario que tiene autorización para iniciar sesión en la consola administrativa de IBM WebSphere Application Server. Este usuario debe tener el rol de agente en el servidor de aplicaciones.
was.wsadmin.password	Especifica la contraseña que corresponde al usuario especificado en la propiedad `was.wsadmin.username`.
was.client.props	Especifica si se deben recuperar los valores de seguridad de un archivo de propiedades del cliente. Los valores posibles son `True` y `False`.
Valores de WebSphere Application Server	
was.appserver.profile.name	Especifica el nombre del perfil del servidor de aplicaciones que desea configurar. No se utiliza para WebSphere Application Server Liberty.
was.appserver.home	Especifica el directorio de inicio de WebSphere Application Server.
was.appserver.cell.name	Especifica el nombre de célula de WebSphere Application Server. No se utiliza para WebSphere Application Server Liberty.
was.appserver.node.name	Especifica el nombre de nodo de WebSphere Application Server. No se utiliza para WebSphere Application Server Liberty.
Valores de instancia de tiempo de ejecución de WebSphere Application Server	
was.appserver.server.name	Especifica la instancia de servidor de aplicaciones dentro del perfil de servidor de aplicación que se va a configurar. **Consejo:** • El archivo de respuestas silencioso puede tener varias instancias de esta propiedad • Cuando añada un segundo servidor, elimine el comentario del segundo servidor (es decir, #[SERVER]) y añada el nombre del servidor.

Tabla 223. Propiedades disponibles para la ejecución del programa de utilidad de configuración en modalidad silenciosa (continuación)

Propiedad	Comentario
tema.serveralias	Especifica el nombre del nodo en la interfaz de usuario de supervisión que contiene la información de supervisión para esta instancia de servidor de aplicaciones. El valor predeterminado es el nombre del nodo combinado con el nombre del servidor. **Importante:** El alias puede contener solo los caracteres siguientes: A-Z, a-z, subrayado (_), guión (-) y punto (.). No utilice otros caracteres en el alias. **Consejo:** El archivo de respuestas silencioso puede tener varias instancias de esta propiedad. **Recuerde:** Al cambiar el alias de servidor se cambia el nombre de la instancia de agente que se ha registrado con la Consola de Cloud APM. Si no es la primera vez que configura el recopilador de datos y ha cambiado el alias de servidor, debe borrar algunos archivos de la memoria caché. Para obtener instrucciones detalladas, consulte Borrar los archivos de memoria caché con los nombres de servidor antiguos.

Configuración manual del recopilador de datos si fallan los programas de utilidad de configuración
Si no puede utilizar el programa de utilidad de configuración interactiva proporcionado para configurar el recopilador de datos para el Agente de WebSphere Applications, puede configurar manualmente el recopilador de datos en WebSphere Administrative Console.

Antes de empezar

- Instale la Agente de WebSphere Applications.
- Averigüe el directorio de inicio del recopilador de datos, que es necesario para la configuración del recopilador de datos. El valor predeterminado es `/opt/ibm/apm/agent/yndchome/7.3.0.14.08` en sistema Linux y UNIX o `C:\IBM\APM\dchome\7.3.0.14.08` en sistemas Windows.
- Si desea configurar el recopilador de datos para un servidor Liberty, averigüe el directorio de inicio del servidor Liberty. Por ejemplo, `/opt/ibm/was/liberty/usr/servers/defaultServer`.
- Asegúrese de que un archivo llamado `itcam_wsBundleMetaData.xml` existe en la carpeta *dir_inicio_dc*`/runtime/wsBundleMetaData` y de que tiene el contenido siguiente. Si la carpeta o el archivo no existen, créelo manualmente.

  Recuerde: El valor *dir_plugins_dentro_inicio_dc* se debe establecer en la vía de acceso absoluta de la carpeta `plugins` dentro del directorio inicial del recopilador de datos. El valor predeterminado es `/opt/ibm/apm/agent/yndchome/7.3.0.14.08/plugins` en sistemas Linux y UNIX o `C:\IBM\APM\dchome\7.3.0.14.08\plugins` en sistemas Windows.

```
<bundles>
  <directory path="dir_plugins_dentro_inicio_dc">
      <bundle>com.ibm.tivoli.itcam.bundlemanager_7.2.0.jar</bundle>
  </directory>
  <directory path="dir_plugins_dentro_inicio_dc">
      <bundle>com.ibm.tivoli.itcam.classicsca_7.2.0.jar</bundle>
  </directory>
  <directory path="dir_plugins_dentro_inicio_dc">
      <bundle>com.ibm.tivoli.itcam.toolkitsca.classicsca_7.2.0.jar</bundle>
  </directory>
</bundles>
```

Acerca de esta tarea

Importante:

- Debe realizar cambios manuales en la configuración de WebSphere Application Server para los recopiladores de datos como el usuario administrativo de WebSphere.
- Debe ser un administrador experimentado de WebSphere para realizar cambios manuales en WebSphere Application Server para la recopilación de datos. Cualquier error en el cambio de configuración manual puede dar lugar a que el servidor de aplicaciones no se inicie.
- Tras configurar manualmente el recopilador de datos para supervisar las instancias de servidor de aplicaciones, no puede utilizar el programa de utilidad de desconfiguración para desconfigurar el recopilador de datos. Deberá desconfigurar manualmente el recopilador de datos.

Procedimiento

- Para configurar manualmente el recopilador de datos de WebSphere Application Server, consulte "Configuración manual del recopilador de datos para WebSphere Application Server tradicional" en la página 887.
- Para configurar manualmente el recopilador de datos de Liberty Server, consulte "Configuración manual del recopilador de datos para WebSphere Application Server Liberty" en la página 889.

Configuración manual del recopilador de datos para WebSphere Application Server tradicional

Procedimiento

1. Inicie la sesión en la consola administrativa de WebSphere como administrador.
2. En el panel de navegación, pulse **Servidores**, expanda **Tipos de servidores** y pulse **Servidores de aplicaciones WebSphere**.
3. En la sección **Infraestructura de servidor** de la pestaña Configuración, expanda **Java y gestión de proceso** y pulse **Definición de procesos**.
4. En la sección **Propiedades adicionales**, pulse **Máquina virtual Java**.
5. En el campo **Argumentos de JVM genéricos**, añada las siguientes entradas.

   ```
   -agentlib:am_ibm_16=${WAS_SERVER_NAME} -Xbootclasspath/p:${ITCAMDCHOME}/
   toolkit/lib/bcm-bootstrap.jar -Djava.security.policy=${ITCAMDCHOME}/itcamdc/
   etc/datacollector.policy -verbosegc
   ```

   Al añadir las entradas, tenga en cuenta lo siguiente:

   - Todas las entradas deben estar en una sola línea.
   - Separe los distintos argumentos con espacios antes del signo menos (-) y no utilice espacios en ninguna otra parte.
6. Pulse **Aplicar** y guarde los cambios en la configuración maestra.
   - Si no está en un entorno de despliegue de red, pulse **Guardar**.
   - Si está en un entorno de despliegue de red, asegúrese de que **Sincronizar cambios con nodos** está seleccionado en las opciones de **Preferencias de consola** y luego pulse **Guardar**.
7. En el panel de navegación, pulse **Servidores**, expanda **Tipos de servidores**, pulse **Servidores de aplicaciones WebSphere** y pulse el nombre del servidor.
8. En la pestaña Configuración, vaya a **Infraestructura de servidor** > **Java y gestión de procesos** > **Definición de procesos** > **Entradas de entorno**.
9. Dependiendo del sistema operativo, la plataforma de hardware y la JVM del servidor de aplicaciones, establezca la siguiente entrada de entorno.

Tabla 224. Entrada de entorno

Plataforma	Nombre de entrada de entorno	Valor de entrada de entorno
AIX R6.1 (JVM de 64 bits)	LIBPATH	/lib:${ITCAMDCHOME}/ toolkit/lib/aix536

Tabla 224. Entrada de entorno (continuación)		
Plataforma	**Nombre de entrada de entorno**	**Valor de entrada de entorno**
AIX R7.1 (JVM de 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/aix536`
Solaris 10 (JVM de 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/sol296`
Solaris 11 (JVM de 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/sol296`
Linux Intel R2.6 (JVM de 32 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/li6263`
Linux x86_64 R2.6 (JVM de 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/lx8266`
Linux on Power Little Endian (JVM de 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/lpl266`
Linux on System z (JVM de 32 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/ls3263`
Linux on System z (JVM de 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/ls3266`
Windows (JVM de 32 bits)	PATH	`/lib;${ITCAMDCHOME}/toolkit/lib/win32`
Windows (JVM de 64 bits)	PATH	`/lib;${ITCAMDCHOME}/toolkit/lib/win64`

10. Pulse **Aplicar** y guarde los cambios en la configuración maestra.
    - Si no está en un entorno de despliegue de red, pulse **Guardar**.
    - Si está en un entorno de despliegue de red, asegúrese de que **Sincronizar cambios con nodos** está seleccionado en las opciones de **Preferencias de consola** y luego pulse **Guardar**.
11. En el panel de navegación, pulse **Entorno** > **Variables de WebSphere**.
12. Especifique el ámbito del nivel de servidor adecuado y añada la variable *ITCAMDCHOME*. Establezca el valor de la variable *ITCAMDCHOME* en el directorio de inicio del recopilador de datos. Por ejemplo, `/opt/ibm/apm/agent/yndchome/7.3.0.14.08`.
13. Pulse **Aplicar** y guarde los cambios en la configuración maestra.
    - Si no está en un entorno de despliegue de red, pulse **Guardar**.
    - Si está en un entorno de despliegue de red, asegúrese de que **Sincronizar cambios con nodos** está seleccionado en las opciones de **Preferencias de consola** y luego pulse **Guardar**.
14. Reinicie el servidor de aplicaciones.

Resultados

Ahora puede comprobar los datos del Agente de WebSphere Applications en la Consola de Cloud APM después de añadir este componente de aplicación a las aplicaciones. Si desea instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009. Para obtener instrucciones acerca de cómo añadir o editar una aplicación, consulte la sección "Gestión de aplicaciones" en la página 1133.

Qué hacer a continuación

Tras configurar manualmente el recopilador de datos, no puede utilizar el programa de utilidad `unconfig` suministrado para desconfigurar el recopilador de datos. Desconfigure manualmente el

recopilador de datos. Para obtener instrucciones, consulte “Desconfiguración manual del recopilador de datos” en la página 160.

Configuración manual del recopilador de datos para WebSphere Application Server Liberty

Procedimiento

1. Vaya al directorio inicial del servidor Liberty. Por ejemplo, `/opt/ibm/wlp/usr/servers/defaultServer`.
2. Edite el archivo `jvm.options` añadiendo los parámetros siguientes, donde *inicio_dc* es el directorio inicial del recopilador de datos y *nombre_servidor* es el nombre del servidor Liberty. Si el archivo `jvm.options` no existe, créelo con un editor de texto.

   ```
   -agentlib:am_ibm_16=nombre_servidor
   –Xbootclasspath/p:inicio_dc/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=inicio_dc/itcamdc/etc/datacollector.policy
   -verbosegc
   ```

   Al añadir las entradas, tenga en cuenta lo siguiente:

   - Cada entrada debe estar en una sola línea.
   - Sustituya *nombre_servidor* por el nombre de servidor de Liberty real. Por ejemplo, `defaultServer`.
   - Sustituya *inicio_dc* por el directorio de inicio real del recopilador de datos. Por ejemplo, `/opt/ibm/apm/agent/yndchome/7.3.0.14.08`.
3. Abra el archivo `server.env` del mismo directorio y añada la siguiente vía de acceso a la entrada de entorno en función del sistema operativo, donde *inicio_dc* es el directorio de inicio del recopilador de datos. Si el archivo `server.env` no existe, créelo con un editor de texto.

   Tabla 225. Entrada de entorno

Plataforma	**Nombre de entrada de entorno**	**Valor de entrada de entorno**
AIX R6.1 (JVM de 64 bits)	LIBPATH	`/lib:`*inicio_dc*`/toolkit/lib/aix536`
AIX R7.1 (JVM de 64 bits)	LIBPATH	`/lib:`*inicio_dc*`/toolkit/lib/aix536`
Solaris 10 (JVM de 64 bits)	LIBPATH	`/lib:`*inicio_dc*`/toolkit/lib/sol296`
Solaris 11 (JVM de 64 bits)	LIBPATH	`/lib:`*inicio_dc*`/toolkit/lib/sol296`
Linux x86_64 R2.6 (JVM de 64 bits)	LD_LIBRARY_PATH	`/lib:`*inicio_dc*`/toolkit/lib/lx8266`
Linux Intel R2.6 (JVM de 32 bits)	LD_LIBRARY_PATH	`/lib:`*inicio_dc*`/toolkit/lib/li6263`
Windows (JVM de 32 bits)	PATH	`/lib;`*inicio_dc*`/toolkit/lib/win32`
Windows (JVM de 64 bits)	PATH	`/lib;`*inicio_dc*`/toolkit/lib/win64`

4. Abra el archivo `server.xml` en el mismo directorio y añada las líneas siguientes para habilitar la característica de supervisión:

   ```
   <featureManager>
                 <feature>webProfile-7.0</feature>
                 <feature>monitor-1.0</feature>
                 <feature>usr:itcam-730.140</feature>
      </featureManager>
   ```

5. Reinicie el servidor Liberty.

Resultados
Ahora puede comprobar los datos del Agente de WebSphere Applications en la Consola de Cloud APM después de añadir este componente de aplicación a las aplicaciones. Si desea instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009. Para obtener instrucciones acerca de cómo añadir o editar una aplicación, consulte la sección "Gestión de aplicaciones" en la página 1133.

Qué hacer a continuación

Tras configurar manualmente el recopilador de datos, no puede utilizar el programa de utilidad `unconfig` suministrado para desconfigurar el recopilador de datos. Desconfigure manualmente el recopilador de datos. Para obtener instrucciones, consulte "Desconfiguración manual del recopilador de datos" en la página 160.

(Coexistencia de agentes) Configuración del Agente de WebSphere Applications y del recopilador de datos
En el entorno de coexistencia de agentes donde están instalados el Agente de WebSphere Applications e ITCAM Agent for WebSphere Applications, debe realizar algunas tareas de configuración adicionales para el agente y seguir un procedimiento diferente para configurar el recopilador de datos.

Acerca de esta tarea

En el entorno de coexistencia de agentes, debe configurar sólo un recopilador de datos para enviar datos tanto al Agente de WebSphere Applications como a ITCAM Agent for WebSphere Applications. Ambos agentes deben utilizar puertos diferentes para escuchar las solicitudes del recopilador de datos.

Procedimiento

1. Si el recopilador de datos de ITCAM Agent for WebSphere Applications, que está instalado en la infraestructura de IBM® Tivoli® Monitoring antigua, existe en el entorno, desinstálelo.
2. Instale el Agente de WebSphere Applications suministrado en IBM Cloud Application Performance Management 8.1.3 o posterior. Con ello se asegurará de que esté instalado el recopilador de datos de la versión 7.3.0.11.0 o posterior, que está soportado para la coexistencia de agentes.
3. Asegúrese de que el ID de usuario que va a configurar el recopilador de datos y el ID de usuario que ha instalado el servidor de aplicaciones tienen los privilegios de usuario adecuados requeridos por el agente. Si desea más instrucciones, consulte "Comprobación de los requisitos de acceso de usuario" en la página 866.
4. Asegúrese de que el Agente de WebSphere Applications e ITCAM Agent for WebSphere Applications estén utilizando números de puerto distintos para la escucha de las solicitudes procedentes del recopilador de datos. Los números de puerto deben ser exclusivos, lo cual implica que no pueden ser utilizados por ningún otro componente del entorno. Configure el agente de nuevo para cambiar el puerto, si es necesario.
   - Encontrará información sobre cómo configurar el Agente de WebSphere Applications en "Configuración del Agente de WebSphere Applications" en la página 891.
   - Para obtener información sobre cómo configurar el ITCAM Agent for WebSphere Applications, consulte la documentación de ITCAM for Application Diagnostics o ITCAM for Applications.
5. Utilice el programa de utilidad de configuración proporcionado para configurar el recopilador de datos. Para obtener instrucciones, consulte "Configuración del recopilador de datos para el entorno de coexistencia de agentes" en la página 892.

   Consejo: si está familiarizado con la configuración del recopilador de datos, también puede configurarlo en modalidad silenciosa. Para obtener instrucciones, consulte "Configuración del recopilador de datos en modalidad silenciosa" en la página 878.

Configuración del Agente de WebSphere Applications

En el entorno de coexistencia de agentes, el Agente de WebSphere Applications y el ITCAM Agent for WebSphere Applications comparten el recopilador de datos. Ambos agentes deben utilizar puertos diferentes para escuchar las solicitudes del recopilador de datos. Debe configurar el agente para cambiar el puerto, si es necesario.

Acerca de esta tarea

- En sistemas Linux o AIX, puede configurar el agente de forma interactiva ejecutando el script de configuración y luego respondiendo a las solicitudes, o de forma silenciosa mediante la creación de un archivo de respuestas silencioso y ejecutando el script de configuración sin interacción.
- En sistemas Windows, puede configurar el agente mediante la creación de un archivo de respuestas silencioso y ejecutando el script de configuración, o con el programa de utilidad Gestionar servicios de supervisión proporcionado. Para obtener información sobre cómo iniciar Gestionar servicios de supervisión en sistemas Windows, consulte "Utilización de la ventana de IBM Cloud Application Performance Management en sistemas Windows" en la página 189.

Procedimiento

- Para configurar el agente mediante la edición del archivo de respuestas silencioso y la ejecución del script sin interacción, siga estos pasos:
  a) Cree un archivo `.txt` como el archivo de respuestas silencioso.
  b) Especifique los parámetros siguientes en el archivo de respuestas silencioso. La sintaxis es *nombre_parámetro=valor_parámetro*.

  configure_type
  Especifica el tipo de configuración. Este parámetro es necesario.

  El valor válido es `tema_configure` para configuración de agente.

  KYN_ALT_NODEID
  Especifica el ID de nodo alternativo para identificar el agente. Este parámetro es necesario.

  El valor válido es una serie alfanumérica de hasta 24 caracteres.

  KYN_PORT
  Especifica el puerto de escucha que utiliza el agente. Este es el socket TCP que el agente utiliza para escuchar las solicitudes de conexión del recopilador de datos. Este parámetro es necesario.

  El valor predeterminado es 63335.

  Recuerde: En el entorno de coexistencia de agentes, asegúrese de que el número de puerto que ha especificado aquí no lo esté utilizando el ITCAM Agent for WebSphere Applications.

  Por ejemplo, añada las líneas siguientes en el archivo `.txt` que ha creado.

```
configure_type=tema_configure
KYN_ALT_NODEID=WASAgent
KYN_PORT=63335
```

  c) Guarde y cierre el archivo, y especifique el mandato siguiente para ejecutar el script de configuración:

  – Linux AIX *dir_instalación*/bin/was-agent.sh config *vía_acceso_a_archivo_respuestas*

  – Windows *dir_instalación*\bin\was-agent.bat config *vía_acceso_a_archivo_respuestas*

  Donde *dir_instalación* es el directorio de instalación del agente. El valor predeterminado es `C:\IBM\APM` en sistemas Windows, `/opt/ibm/apm/agent` en sistemas Linux y sistemas AIX.

  d) Una vez completada la configuración, reinicie el Agente de WebSphere Applications si no se está ejecutando, con el mandato siguiente:

- Linux AIX *dir_instalación*/bin/was-agent.sh start
- Windows *dir_instalación*\bin\was-agent.bat start

- Para configurar el agente mediante la ejecución del script y las respuestas a las solicitudes, siga estos pasos:
  a) Desde la línea de mandatos, vaya al directorio *dir_instalación*/bin, donde *dir_instalación* es el directorio de instalación de agente.

     El valor predeterminado es /opt/ibm/apm/agent en sistemas Linux y sistemas AIX.
  b) Ejecute el script de configuración desde el directorio:

```
./was-agent.sh config
```

  c) Cuando se le solicite, especifique 1 y pulse Intro para editar los valores para el agente de supervisión de Agente de WebSphere Applications.
  d) Pulse Intro hasta que se le solicite un ID de nodo alternativo para identificar el agente de supervisión.
  e) Proporcione el ID de nodo y pulse Intro. El formato válido del ID de nodo es una serie alfanumérica con un máximo de 24 caracteres.
  f) Cuando se le solicite el número de puerto, proporcione el puerto utilizado por el agente para escuchar las solicitudes de conexión del recopilador de datos y pulse Intro.

     Recuerde: Para el entorno de coexistencia de agentes, asegúrese de que el puerto especificado no lo esté utilizando el ITCAM Agent for WebSphere Applications.
  g) Una vez completada la configuración, reinicie el Agente de WebSphere Applications.

Resultados
Ha configurado el Agente de WebSphere Applications.

Qué hacer a continuación
A continuación, debe configurar el recopilador de datos. Al configurar el recopilador de datos, se le solicitará que proporcione el número de puerto que ha configurado para el Agente de WebSphere Applications y ITCAM Agent for WebSphere Applications. Para obtener instrucciones, consulte “Configuración del recopilador de datos para el entorno de coexistencia de agentes” en la página 892.

Configuración del recopilador de datos para el entorno de coexistencia de agentes
Si en su entorno tiene tanto el Agente de WebSphere Applications como el ITCAM Agent for WebSphere Applications, puede configurar sólo un recopilador de datos para ambos agentes.

Antes de empezar
Asegúrese de haber completado otros pasos que se indican en “(Coexistencia de agentes) Configuración del Agente de WebSphere Applications y del recopilador de datos” en la página 890.

Acerca de esta tarea

Utilice el programa de utilidad de configuración interactiva proporcionado para configurar el recopilador de datos para un entorno donde existen el Agente de WebSphere Applications y el ITCAM Agent for WebSphere Applications y ambos comparten el recopilador de datos.

Limitación: La integración del recopilador de datos con los siguientes componentes o productos no está soportada para ITCAM Agent for WebSphere Applications:

- Servidor de gestión de ITCAM for Application Diagnostics
- ITCAM for Transactions
- Tivoli Performance Viewer

Recuerde: La supervisión de WebSphere Application Server Liberty no está soportada por ITCAM Agent for WebSphere Applications. Para supervisar WebSphere Application Server Liberty, utilice el Agente de WebSphere Applications solamente. Para obtener información sobre la configuración del recopilador de datos para la supervisión de Liberty, consulte "Configuración interactiva del recopilador de datos" en la página 870 o "Configuración del recopilador de datos en modalidad silenciosa" en la página 878.

Procedimiento

1. Inicie la sesión en el sistema con el ID de usuario utilizado para instalar el servidor de aplicaciones.
2. Desde la línea de mandatos, vaya al directorio `bin` en el directorio *dir_inicio_dc*. El directorio *dir_inicio_dc* es el siguiente:
   - Windows *dir_instal*\dchome\7.3.0.14.08
   - Linux AIX *dir_instal*/yndchome/7.3.0.14.08
3. Ejecute el siguiente mandato para iniciar el programa de utilidad de configuración:
   - Windows `config.bat`
   - Linux AIX `./config.sh`

   El programa de utilidad de configuración se inicia y muestra las direcciones IP de todas las tarjetas de red que se encuentran en el sistema local.
4. Especifique el número que corresponda a la dirección IP que se va a utilizar y pulse Intro.

   El programa de utilidad de configuración muestra los directorios de inicio de WebSphere Application Server que se han descubierto en el sistema.
5. Cuando se le solicite el directorio de inicio del servidor de aplicaciones, especifique el número que corresponde a un directorio de inicio de WebSphere Application Server o una vía de acceso completa a un directorio de inicio del servidor de aplicaciones y pulse Intro.

   El programa de utilidad de configuración muestra todos los perfiles de servidor de aplicaciones descubiertos bajo el directorio de inicio especificado.
6. Cuando se le solicite el perfil del servidor de aplicaciones a configurar, especifique el número que corresponde al perfil de WebSphere Application Server y pulse Intro.

   El programa de utilidad de configuración indica si WebSphere Global Security está habilitada para el perfil de WebSphere Application Server que ha especificado. Si la seguridad global no está habilitada, vaya al paso "8" en la página 893.
7. Especifique si se deben recuperar los valores de seguridad de un archivo de propiedades del cliente. Especifique 1 para permitir que el programa de utilidad de configuración recupere el nombre de usuario y la contraseña del archivo de propiedades de cliente correspondiente. En caso contrario, especifique 2 para indicar el nombre de usuario y la contraseña del administrador de WebSphere.

   El recopilador de datos se comunica con los Servicios administrativos de WebSphere utilizando invocación a método remoto (RMI) o el protocolo SOAP. Si la seguridad global está habilitada para un perfil, debe especificar el ID de usuario y la contraseña de un usuario que tenga autorización para iniciar sesión en la consola administrativa de WebSphere Application Server para el perfil del servidor de aplicaciones. O bien puede cifrar el nombre de usuario y la contraseña y almacenarlos en archivos de propiedades de cliente antes de configurar el recopilador de datos. Debe utilizar el archivo `sas.client.props` para una conexión RMI o el archivo `soap.client.props` para una conexión SOAP.
8. Cuando se le solicite el nombre de host de la consola de administración de WebSphere, pulse Intro para aceptar el valor predeterminado o especifique el nombre de host o la dirección IP de la consola de administración de WebSphere. El valor predeterminado es `localhost`.
9. Cuando el programa de utilidad de configuración muestre todas las instancias de servidor que todavía no están configuradas para la recopilación de datos, seleccione una o varias instancias de servidor de aplicaciones de la lista. Especifique el número correspondiente a la instancia de servidor de aplicaciones para configurar la recopilación de datos o especifique un asterisco (*) para configurar todas las instancias de servidor de aplicaciones para la recopilación de datos, y pulse Intro. Para

especificar un subconjunto de servidores, especifique los números, separados por comas, que representan los servidores.
Por ejemplo, `1,2,3`.

Recuerde:

- Para un entorno autónomo, las instancias de servidor de aplicaciones deben estar ejecutándose durante la configuración.
- En un entorno de Network Deployment, el gestor de despliegue debe estar en ejecución.
- Asegúrese de que las instancias de servidor de aplicaciones que seleccione son los servidores reales que alojan las aplicaciones o los servicios que desea supervisar.

El programa de utilidad de configuración proporciona una opción para integrar el recopilador de datos para el Agente de WebSphere Applications.

10. En la sección **Integración con Agente para aplicaciones WebSphere**, especifique que desea integrar el recopilador de datos con el agente de supervisión. Debe especificar 1 para seleccionar esta opción de integración y, a continuación, pulse Intro.

    El servidor seleccionado se registrará para la supervisión de recursos PMI.
11. Especifique si desea configurar el recopilador de datos dentro de la instancia de servidor de aplicaciones. Debe especificar 1 para sí y, a continuación, pulsar Intro.
12. Especifique si se debe habilitar el recopilador de datos para datos de diagnóstico. Escriba 1 para sí o 2 para no.
13. Cuando se le solicite el nombre de host del componente de agente de supervisión V8, especifique el nombre de host o la dirección IP del Agente de WebSphere Applications o acepte el valor predeterminado.
14. Cuando se le solicite el número de puerto del agente de supervisión V8, especifique el número de puerto utilizado por el Agente de WebSphere Applications.

    Recuerde: es posible que el valor predeterminado no sea el adecuado para utilizar si lo utiliza otro componente. Debe asegurarse de que el puerto especificado no sea utilizado por ningún otro componente en su entorno.
15. Especifique que desea configurar el agente de supervisión V6. Especifique 1 para configurar el ITCAM Agent for WebSphere Applications y pulse Intro.
16. Cuando se le solicite el nombre de host o la dirección IP del agente de supervisión V6, especifique el nombre de host o la dirección IP del ITCAM Agent for WebSphere Applications.
17. Cuando se le solicite el número de puerto del agente de supervisión V6, especifique el número de puerto utilizado por el componente del agente de supervisión del ITCAM Agent for WebSphere Applications.

    Recuerde: es posible que el valor predeterminado no sea el adecuado para utilizar si lo utiliza otro componente. Debe asegurarse de que el puerto especificado no sea utilizado por ningún otro componente en su entorno.
18. Cuando se le solicite el alias de servidor, no utilice el valor predeterminado y especifique un alias de servidor exclusivo que desee utilizar. Si está configurando varias instancias de servidor de aplicaciones, el programa de utilidad de configuración le solicitará un alias para cada instancia.

    Importante: El alias puede contener solo los caracteres siguientes: `A-Z`, `a-z`, subrayado (`_`), guión (`-`) y punto (`.`). No utilice otros caracteres en el alias.

    El alias de servidor es el primer calificador del nombre de instancia de agente (conocido también como MSN) que se visualiza en la Consola de Cloud APM. El valor predeterminado es el nombre del nodo combinado con el nombre del servidor. Por ejemplo, el alias **node1server1** indica el servidor denominado **server1** en el nodo denominado **node1**.
19. Cuando se le solicite el número de puerto TCP/IP para la supervisión de recursos PMI, pulse Intro para aceptar el valor predeterminado o especifique un número nuevo. El puerto predeterminado es 63355.

El puerto se utiliza para la comunicación interna entre los componentes que se ejecutan en el mismo host. Si el puerto predeterminado está en uso, establezca un número diferente.

20. En la sección **Soporte para el rastreo de transacciones**, especifique si debe habilitarse el rastreo de transacciones. Especifique 1 para sí, o especifique 2 para no y vaya al paso 22.

    Recuerde: para ver información de rastreo de transacciones, debe habilitar el rastreo de transacciones en la página de Configuración de agente de la Consola de Cloud APM.
21. Acepte el nombre de host predeterminado o la dirección IP de la extensión de infraestructura de transacciones, que es un componente interno del Agente de WebSphere Applications que recopila métricas del recopilador de datos.
22. Acepte el número de puerto predeterminado que utiliza el recopilador de datos para conectase a la extensión de infraestructura de transacciones. El valor predeterminado es 5457.
23. Especifique si se debe integrar el recopilador de datos con Application Performance Diagnostics Lite. Pulse Intro para aceptar el valor predeterminado, No.
24. En la sección **Configuración avanzada**, especifique si desea cambiar la vía de acceso de registro de recogida de basura. Especifique 1 para seleccionar una vía de acceso del registro de recogida de basura. De lo contrario, especifique 2 y vaya al paso "26" en la página 895.
25. Especifique la vía de acceso de registro de recogida de basura. Especifique un nombre de archivo con su vía de acceso completa.

    Por ejemplo, si especifica `gc.log` como nombre de archivo, el nombre real se establece en *`nombre_perfil.nombre_célula.nombre_nodo.nombre_servidor`*`.gc.log` para cada instancia de servidor de aplicaciones configurada.

    Importante: En la vía de acceso del registro de recogida de basura, puede utilizar variables de WebSphere como por ejemplo `${SERVER_LOG_ROOT}`. No obstante, no utilice plantillas, como `%pid`.
26. En la sección **Resumen de configuración del recopilador de datos**, revise el resumen de la configuración del recopilador de datos que se aplicará a las instancias de servidor de aplicaciones especificadas. Si es necesario, modifique los valores de configuración.
27. Especifique a para aceptar los cambios.
28. Cuando se le solicite, especifique si desea crear una copia de seguridad de la configuración actual. Especifique 1 para crear una copia de seguridad de la configuración actual. De lo contrario, especifique 2.
29. Reinicie las instancias del servidor de aplicaciones cuando se lo indique el programa de utilidad de configuración.
    a) Vaya al directorio `bin` bajo el directorio de inicio del perfil de servidor de aplicaciones. Por ejemplo, `opt/IBM/WebSphere/AppServer/profiles/`*`nombre_perfil`*`/bin`.
    b) Detenga el servidor de aplicaciones especificando el mandato **`stopServer`** en la consola de mandatos.
       - Linux AIX `./stopServer.sh` *`nombre_servidor`*
       - Windows `stopServer.bat` *`nombre_servidor`*
    c) Cuando se le solicite, especifique el ID de usuario y la contraseña del administrador de la consola de administración de WebSphere.
    d) Inicie de nuevo el servidor de aplicaciones especificando el mandato **`startServer`** en la consola de mandatos.
       - Linux AIX `./startServer.sh` *`nombre_servidor`*
       - Windows `startServer.bat` *`nombre_servidor`*

    La configuración del recopilador de datos entra en vigor una vez reiniciado el servidor de aplicaciones.
30. Inicie la sesión en Consola de Cloud APM para ver los datos en los paneles de instrumentos.

a) Acceda a la consola mediante el enlace que se proporciona en el correo electrónico que le informa de que el servicio está preparado. También puede acceder a la consola desde el sitio web IBM Marketplace. Para obtener instrucciones detalladas, consulte "Inicio de la Consola de Cloud APM" en la página 1009.

b) Utilice el editor de aplicaciones para añadir el servidor de aplicaciones supervisado al Panel de instrumentos del rendimiento de aplicaciones. Puede añadirlo como componente nuevo a la aplicación existente o crear una aplicación para que contenga este componente.

Para obtener más información sobre el editor de aplicaciones, consulte "Gestión de aplicaciones" en la página 1133.

Qué hacer a continuación

- Si el ID de usuario actual utilizado para configurar el recopilador de datos no es el mismo ID del usuario que ejecuta el servidor de aplicaciones, compruebe que el ID de usuario para configurar el recopilador de datos tenga permisos de lectura y escritura sobre los directorios `runtime` y `logs` del directorio de inicio del recopilador de datos. Estos dos subdirectorios los crea el ID del usuario que ejecuta el servidor de aplicaciones cuando éste se reinicia.
- Para Agente de WebSphere Applications, inicie la sesión en la Consola de Cloud APM para ver los datos de supervisión en los paneles de instrumentos. Para ITCAM Agent for WebSphere Applications, inicie la sesión en Tivoli Enterprise Portal para ver los datos. Si los datos de supervisión no están disponibles de inmediato, reinicie el agente de supervisión ejecutando los mandatos siguientes:
  - Windows

    ```
    cd dir_instalación\bin
    was-agent.bat stop
    was-agent.bat start
    ```

  - Linux AIX

    ```
    cd dir_instalación/bin
    ./was-agent.sh
    stop
    ./was-agent.sh start
    ```

- Al cambiar el alias de servidor se cambia el nombre de la instancia de agente que se ha registrado con la Consola de Cloud APM. Si no es la primera vez que configura el recopilador de datos y ha cambiado el alias de servidor, debe borrar algunos archivos de la memoria caché siguiendo estos pasos:
  1. Detenga el agente de supervisión si se está ejecutando.
  2. Abra el archivo *nombre_host*`_yn.xml` en el directorio siguiente con un editor de texto, donde *nombre_host* es el nombre del host en el que el está instalado el Agente de WebSphere Applications o ITCAM Agent for WebSphere Applications.
     - Windows *dir_instalación*`\TMAITM6_x64` (el valor predeterminado es `C:\IBM\APM\TMAITM6_x64` para Agente de WebSphere Applications o `C:\IBM\ITM\TMAITM6_x64` para ITCAM Agent for WebSphere Applications)
     - Linux AIX *dir_instalación*`/config` (el valor predeterminado es `/opt/ibm/apm/agent/config` para Agente de WebSphere Applications o `/opt/ibm/itm/agent/config` para ITCAM Agent for WebSphere Applications)
  3. Busque la línea que empieza con la serie siguiente y contiene el nombre de servidor anterior. Por ejemplo, `was85.win4net01Cell02.win4net01Node02.AppSrv01.server1`, donde `server1` es el nombre anterior del servidor de aplicaciones.

     ```
     <!ENTITY cód_producto_was.nombre_célula.nombre_nodo.nombre_perfil.nombre_servidor
     ```

     donde *cód_producto_was* es el código de producto de WebSphere Application Server; *nombre_célula* es el nombre de la célula; *nombre_nodo* es el nombre de nodo; *nombre_perfil* es el nombre de perfil del servidor de aplicaciones; *nombre_servidor* es el nombre anterior del servidor de aplicaciones.

4. Busque el archivo .XML que se indica en la línea dentro del directorio actual y suprima el archivo.
5. Elimine la línea que ha localizado en el paso 3 en el archivo *nombre_host*_yn.xml.
6. Al final del archivo *nombre_host*_yn.xml, elimine la línea que contiene los nombres de servidor anteriores.
7. Guarde los cambios y cierre el archivo.
8. Reinicie el agente de supervisión.

Reconfiguración del recopilador de datos si cambia el tipo de oferta en Servidor de Cloud APM
Si ha cambiado el tipo de oferta que ha instalado en el Servidor de Cloud APM de Cloud APM, Base a Cloud APM, Advanced y el Agente de WebSphere Applications se había instalado y configurado con la oferta Cloud APM, Base, para utilizar las prestaciones avanzadas del agente suministradas en la oferta Cloud APM, Advanced, deberá desinstalar el Agente de WebSphere Applications anterior e instalar de nuevo el agente con la oferta Cloud APM, Advanced. Como alternativa, puede volver a configurar el recopilador de datos para que las prestaciones estén disponibles en la nueva oferta.

Acerca de esta tarea

El Agente de WebSphere Applications se configura de forma diferente dependiendo del paquete de agente que se utiliza para instalar el agente. Después de cambiar el tipo de oferta en el Servidor de Cloud APM, tiene dos opciones disponibles para las prestaciones de agente en la nueva oferta:

- Elimine el agente que ha instalado con la oferta anterior y, a continuación, instale el agente en la nueva oferta.
- Vuelva a configurar el recopilador de datos para utilizar las prestaciones en la nueva oferta.

Procedimiento

- Elimine el agente que ha instalado con la oferta anterior y, a continuación, instalar el agente en la nueva oferta.
  a) Desconfigure el recopilador de datos. Para obtener instrucciones, consulte “Agente de WebSphere Applications: Desconfiguración del recopilador de datos” en la página 154.
  b) Desinstale el Agente de WebSphere Applications que ha instalado con el paquete de agente de la oferta anterior. Para obtener instrucciones, consulte “Desinstalación de los agentes” en la página 151.
  c) Instale el Agente de WebSphere Applications con el paquete de agente en la nueva oferta y vuelva a configurar el recopilador de datos. Para obtener instrucciones, consulte “Configuración del recopilador de datos con el programa de utilidad de configuración simple” en la página 867.
- Vuelva a configurar el recopilador de datos para utilizar las prestaciones en la nueva oferta.
  a) Edite el archivo `offering.id` en el directorio de inicio del recopilador de datos cambiando el valor **IOFFERING** por uno de los siguientes valores, en función del nuevo tipo de oferta:

     BASE
     Si el nuevo tipo de oferta es Cloud APM, Base Private.

     ADVANCED
     Si el nuevo tipo de oferta es Cloud APM, Advanced Private.

     El directorio de inicio del recopilador de datos es el siguiente:

     – Windows *dir_instal*\dchome\7.3.0.14.08
     – Linux AIX *dir_instal*/yndchome/7.3.0.14.08

  b) Vuelva a configurar el recopilador de datos para habilitar los diagnósticos, el rastreo de transacciones, o ambos en el recopilador de datos basándose en lo que está soportado en el nuevo tipo de oferta. Para obtener instrucciones sobre cómo configurar el recopilador de datos, consulte “Configuración del recopilador de datos con el programa de utilidad de configuración simple” en la página 867.

c) Reinicie WebSphere Application Server.

d) Desde cualquier página de la Consola de Cloud APM, pulse **Configuración del sistema** > **Configuración del agente** para abrir la página **Configuración del agente**. Asegúrese de que el valor de rastreo de transacciones coincide con las prestaciones disponibles en el nuevo tipo de oferta. Si no es así, actualice el valor.

El valor de rastreo de transacciones debe estar habilitado para Cloud APM, Advanced, pero estar inhabilitado para Cloud APM, Base.

Supervisión de WebSphere Application Server Liberty dentro de un contenedor de Docker
Para supervisar un perfil de Liberty dentro de un contenedor de Docker, debe utilizar el mandato **docker run** con unas pocas opciones para configurar el recopilador de datos antes de que se pueda iniciar WebSphere Application Server Liberty.

Antes de empezar
Debe instalar el Agente de WebSphere Applications en el host de Docker.

Acerca de esta tarea

Cada perfil de Liberty que se ejecuta dentro de un contenedor de Docker requiere un recopilador de datos para recopilar las métricas de recurso, las métricas de transacción y los datos de diagnóstico y, a continuación, transmitir los datos al agente de supervisión que se ejecuta en el host de Docker. Todos los recopiladores de datos configurados en el mismo host de Docker comparten el mismo agente de supervisión en el host.

Procedimiento

Para configurar el recopilador de datos para un contenedor de perfiles de Liberty, realice los pasos siguientes:

1. Cree un archivo de respuestas silencioso `.txt`, especifique las opciones de configuración siguientes en el archivo y guárdelo.

```
tema.host=host_agente
was.appserver.server.name=nombre_perfil_liberty
```

   Donde **tema.host** se utiliza para especificar la dirección IP del host de agente de supervisión; **was.appserver.server.name** se utiliza para especificar el nombre del perfil de Liberty.

   Consejo: Se incluye un ejemplo de archivo de respuestas silencioso (`sample_silent_liberty_config.txt`) en el directorio *<dir_instalación_agente>*`/agent/yndchome/7.3.0.14.08/bin`. Puede crear su propio archivo de respuestas basándose en este archivo de ejemplo.

2. Ejecute el mandato siguiente para iniciar el nuevo contenedor de Docker. Tenga en cuenta que debe aceptar la licencia para completar la configuración estableciendo el parámetro **LICENSE** en `accept`.

```
$docker run -d -e LICENSE=accept \
-e JAVA_HOME=<dir_inicio_java> \
-p <número_puerto>:<número_puerto> \
-v <dir_aplicaciones_web>:<dir_instalación_liberty>/usr/servers/<nombre_perfil_liberty> \
-v <dir_instalación_agente>/agent/yndchome:<dir_instalación_agente>/agent/yndchome
websphere-liberty /bin/bash \
-c "<dir_instalación_agente>/agent/yndchome/<dcversion>/bin/config.sh -silent
<vía_acceso_absoluta_a_archivo_respuestas_silencioso> && <dir_instalación_liberty>/bin/server
run <nombre_perfil_liberty>"
```

   donde:

   - *<dir_inicio_java>* es el directorio del JRE que el perfil de Liberty utiliza. Por ejemplo, `/opt/ibm/java/jre`.
   - *<número_puerto>* es el número de puerto que se utiliza para la comunicación entre el contenedor y el host.

- *<dir_aplicación_web>* es el directorio donde se encuentra la aplicación web.
- *<dir_instalación_liberty>* es el directorio de instalación de WebSphere Application Server Liberty. El valor predeterminado es `/opt/ibm/wlp`.
- *<nombre_perfil_liberty>* es el nombre del perfil de Liberty.
- *<dir_instalación_agente>* es el directorio de instalación del Agente de WebSphere Applications. El valor predeterminado es `/opt/ibm/apm`.
- *<versión>* es el número de versión del recopilador de datos para Agente de WebSphere Applications. Por ejemplo, 7.3.0.14.08.
- *<vía_acceso_absoluta_a_archivo_respuestas_silencioso>* es la vía de acceso absoluta del archivo de respuestas silencioso que ha creado.

Por ejemplo, el mandato siguiente configura el recopilador de datos para el perfil de Liberty llamado newitcam. Tanto el Agente de WebSphere Applications como el perfil de Liberty se instalan en los directorios predeterminados. La versión del agente de supervisión y del recopilador de datos es 7.3.0.14.08.

```
$docker run -d -e LICENSE=accept \
-e JAVA_HOME=/opt/ibm/java/jre \
-p 9082:9082 \
-v /home/kub/liberty-docker/newitcam:/opt/ibm/wlp/usr/servers/newitcam \
-v /opt/ibm/apm/agent/yndchome:/opt/ibm/apm/agent/yndchome websphere-liberty
/bin/bash \
-c "/opt/ibm/apm/agent/yndchome/7.3.0.14.08/bin/config.sh -silent
/opt/ibm/wlp/usr/servers/newitcam/silent_config.txt && /opt/ibm/wlp/bin/server
run newitcam"
```

Resultados
Ahora puede verificar que los datos de Agente de WebSphere Applications se visualizan en la Consola de Cloud APM. La columna **Nombre de celda** en el widget **Información de WAS** muestra el ID del contenedor de Docker donde se ejecuta el perfil de Liberty.

Qué hacer a continuación
Para desconfigurar el recopilador de datos de forma interactiva, utilice el mandato siguiente para iniciar el programa de utilidad de desconfiguración:

```
docker exec -i id_contenedor "<dir_instalación_agente>/yndchome/7.3.0.14.08/bin
/unconfig.sh"
```

Configuración manual del recopilador de datos para supervisar los servidores de clúster dinámico
Puede configurar el recopilador de datos para supervisar las instancias de servidor de aplicaciones en un clúster dinámico añadiendo algunos parámetros de configuración del recopilador de datos a la plantilla de servidor utilizada para crear las instancias de servidor de clúster dinámico. Se trata de un método alternativo para configurar las instancias de servidor de clúster dinámico para crear las plantillas de servidor específicas del Agente de WebSphere Applications.

Acerca de esta tarea

Para configurar el recopilador de datos para la supervisión de clústeres dinámicos, debe crear dos archivos de valores y luego añadir manualmente los valores en la consola de administración de WebSphere para modificar la plantilla de servidor dinámico. El directorio `runtime` se crea automáticamente cuando se inicia el recopilador de datos para la instancia de servidor de aplicaciones. Tenga en cuenta que las actualizaciones en la plantilla de servidor borrarán estos cambios realizados de este modo.

Importante:

- El nombre de clúster no puede contener espacios.
- Debe realizar cambios manuales en la configuración de WebSphere Application Server para los recopiladores de datos como el usuario administrativo de WebSphere.

- Debe ser un administrador experimentado de WebSphere para realizar cambios manuales en WebSphere Application Server para la recopilación de datos. Cualquier error en el cambio de configuración manual puede dar lugar a que el servidor de aplicaciones no se inicie.
- Si configura manualmente el recopilador de datos para supervisar las instancias de servidor de aplicaciones, no puede utilizar el programa de utilidad de desconfiguración para desconfigurar el recopilador de datos. Para desconfigurar el recopilador de datos, debe volver a cambiar manualmente los valores.

Procedimiento

1. Cree el archivo `dcManualInput.txt` en el directorio `runtime` del recopilador de datos.
   Siga las instrucciones de "Creación del archivo dcManualInput.txt" en la página 900.
2. Cree el archivo `itcam_wsBundleMetaData.xml` en el directorio `wsBundleMetaData` del recopilador de datos. Siga las instrucciones de "Creación del archivo itcam_wsBundleMetaData.xml" en la página 903.
3. Utilice la consola de administración de WebSphere para modificar la plantilla de servidor dinámico añadiendo el parámetro de configuración del recopilador de datos. Siga las instrucciones de "Adición de valores con la consola administrativa de WebSphere" en la página 903.

   Consejo: El nombre del miembro de clúster dinámico se utiliza como el calificador medio del nombre de instancia de Agente de WebSphere Applications que se muestra en la Consola de Cloud APM. A veces, el nombre del miembro de clúster puede estar truncado debido al límite de longitud en el nombre de la instancia de agente. En este caso, puede modificar la plantilla de servidor dinámico añadiendo una variable denominada *${MEP_NAME}* y estableciendo el valor en el nombre de la JVM para cada instancia del servidor. A continuación, puede distinguir cada miembro de clúster por el nombre de la JVM real en la Consola de Cloud APM. Si desea más instrucciones, consulte "Opcional: mostrar el nombre de la JVM real para distinguir los miembros del clúster" en la página 907.

Creación del archivo dcManualInput.txt

Acerca de esta tarea

El archivo `dcManualInput.txt` contiene algunos valores necesarios para la configuración inicial del recopilador de datos.

Procedimiento

Para crear el archivo `dcManualInput.txt`, realice los pasos siguientes:

1. Compruebe si existe un archivo llamado *plataforma*`_Template.DCManualInput.txt` en el directorio siguiente. Si no existe, créelo.
   - Linux AIX *dir_instalación*`/yndchome/7.3.0.14.08/runtime`
   - Windows *dir_instalación*`\dchome\7.3.0.14.08\runtime`

   La variable *plataforma* del nombre de archivo indica la arquitectura de sistema operativo, por ejemplo, aix32, xLinux64.

   Puede poner el nombre que desee al archivo. Sin embargo, *plataforma*`_Template.DCManualInput.txt` sigue la convención de nomenclatura cuando se crea el archivo ejecutando el script `configtemplate.sh`. Tendrá que especificar este archivo para la plantilla de servidor con la consola de administración de WebSphere en un paso posterior.
2. Copie el contenido del archivo siguiente en el archivo `.txt` encontrado o creado en el paso anterior.
   - Linux AIX *dir_inicio_dc*`/itcamdc/etc/was/dcInput_manual.properties`
   - Windows *dir_inicio_dc*`\itcamdc\etc\was\dcInput_manual.properties`
3. Edite el contenido del archivo `.txt`. Debe establecer los parámetros de la sección 1 del archivo de acuerdo con las descripciones proporcionadas en la Tabla 226 en la página 901.

Recuerde:

- No cambie los parámetros de la sección 2.
- Algunos de los parámetros de configuración utilizados por el recopilador de datos para crear los directorios de tiempo de ejecución se establecen siempre en none. Esto sucede porque en la supervisión del clúster dinámico, el recopilador de datos utiliza la configuración de la instancia del servidor WebSphere para crear los directorios cuando se inicia la JVM.

Tabla 226. Parámetros de configuración para la Sección 1

Parámetro	**Valor**
local.hostname	La dirección IP o el nombre de dominio totalmente calificado del sistema local.
was.profile.home	El directorio de inicio del perfil. Establézcalo siempre en none para el servidor de clúster dinámico
was.version	Un número de versión corto. Establézcalo siempre en none para el servidor de clúster dinámico
itcam.home	El directorio de inicio del recopilador de datos. Ejemplo: `/opt/ibm/apm/agent/yndchome/7.3.0.14.08`
was.nodename	Nombre de nodo. Establézcalo siempre en none para el servidor de clúster dinámico
was.servername	Nombre de servidor. Establézcalo siempre en none para el servidor de clúster dinámico
was.profilename	Nombre de perfil de WebSphere. Establézcalo siempre en none para el servidor de clúster dinámico

Tabla 226. Parámetros de configuración para la Sección 1 (continuación)

Parámetro	Valor
am.camtoolkit.gpe.dc.operation.mode	Modalidad de operación del recopilador de datos. Los valores válidos son cualquier combinación de `WR`, `TT` y `DE`, donde: **WR** Integra el recopilador de datos con el Agente de WebSphere Applications. **TT** Integra el recopilador de datos con ITCAM for Transactions. **DE** Integra el recopilador de datos con ITCAM Diagnostics Tool. La herramienta se previsualiza en la versión beta de ITCAM for Application Diagnostics. Debe especificar solamente las modalidades de operación necesarias. Por ejemplo, si va a conectar el recopilador de datos con el Agente de WebSphere Applications solamente, especifique `WR`. Separe varias modalidades de operación con una coma. Ejemplo: `am.camtoolkit.gpe.dc.operation.mode=WR, DE`
interp	Código de plataforma. Ejemplo: `interp=win64` o `interp=lx6266`
kwj.serveralias	Nombre de alias de WebSphere Application Server. Establézcalo siempre en none para el servidor de clúster dinámico
temagclog.path	(Opcional) Nombre de vía de acceso del archivo de registro de recogida de basura. Especifique un nombre de archivo exclusivo con la vía de acceso completa. El nombre de vía de acceso no debe incluir espacios.
tema.host	Nombre de host o dirección IP de la estación de trabajo del Agente de WebSphere Applications. Obligatorio si la modalidad de operación incluye Agente de WebSphere Applications (`WR`). Normalmente, el agente de supervisión está instalado en cada sistema donde se ejecuta el recopilador de datos y se puede especificar la dirección de bucle de retorno. Ejemplo: `tema.host=127.0.0.1`
tema.port	Puerto que se va a utilizar para comunicar con el Agente de WebSphere Applications. Obligatorio si la modalidad de operación incluye Agente de WebSphere Applications (`WR`). El valor predeterminado es 63335. Ejemplo: `tema.port=63335`

Tabla 226. Parámetros de configuración para la Sección 1 (continuación)	
Parámetro	**Valor**
tt.connection.string	Nombre de host o dirección IP y el número de puerto del componente de recopilador de transacciones de ITCAM for Transactions en el formato de `tcp:`*`nombre_host`*`(IP):`*`puerto`*. Obligatorio si la modalidad de operación incluye ITCAM for Transactions (TT). Ejemplo: `tt.connection.string=192.38.234.77:5455`

4. Añada las líneas siguientes a la sección 1 del archivo `.txt`.

```
bcm.helper=com.ibm.tivoli.itcam.was.bcm.websphere.DefaultWASBCMHelper
BCM_HELPER=@{bcm.helper}
```

5. Guarde los cambios y cierre el archivo.

Creación del archivo `itcam_wsBundleMetaData.xml`

Acerca de esta tarea

El archivo `itcam_wsBundleMetaData.xml` contiene algunos de los valores necesarios para la configuración inicial del recopilador de datos.

Procedimiento

Para crear este archivo, realice los pasos siguientes:

1. Cree un directorio llamado `wsBundleMetaData` bajo el directorio siguiente:
   - Linux AIX *`dir_instalación`*`/yndchome/7.3.0.14.08/runtime`
   - Windows *`dir_instalación`*`\dchome\7.3.0.14.08\runtime`
2. Cree un archivo llamado `itcam_wsBundleMetaData.xml` y copie el contenido del archivo siguiente en él:
   - Linux AIX *`dir_instalación`*`/yndchome/7.3.0.14.08/itcamdc/etc/was/itcam_wsBundleMetaData_template.xml`
   - Windows *`dir_instalación`*`\dchome\7.3.0.14.08\itcamdc\etc\was\itcam_wsBundleMetaData_template.xml`
3. En el archivo `itcam_wsBundleMetaData.xml`, sustituya la variable *@{CONFIGHOME}* por la vía de acceso completa del directorio de inicio del recopilador de datos.

   El directorio de inicio del recopilador de datos en cada sistema operativo es como se indica a continuación:
   - Linux AIX *`dir_instal`*`/yndchome/7.3.0.14.08`
   - Windows *`dir_instal`*`\dchome\7.3.0.14.08`
4. Coloque el archivo `itcam_wsBundleMetaData.xml` en el directorio `wsBundleMetaData` creado en el paso 1.

Adición de valores con la consola administrativa de WebSphere

Procedimiento

Complete los pasos siguientes para modificar la plantilla de servidor dinámico con la consola administrativa de WebSphere.

1. Inicie la sesión en la consola administrativa de WebSphere.

2. Pulse **Servidores**.
3. Expanda **Clústeres** y seleccione **Clústeres dinámicos**.
4. Pulse el nombre del clúster de servidores dinámico que desea configurar con el recopilador de datos.
5. En la sección **Propiedades adicionales**, pulse **Plantilla de servidor**.
6. En la sección **Infraestructura de servidor**, expanda **Java y gestión de proceso** y pulse **Definición de procesos**.
7. En la sección **Propiedades adicionales**, pulse **Máquina virtual Java**.
8. En el campo **Argumentos de JVM genéricos**, añada las siguientes entradas.

```
-agentlib:am_$jvm-vendor_$jvm-version=${WAS_SERVER_NAME}
-Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
-verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
$platform_Template_DCManualInput.txt
-Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
-Dsun.rmi.transport.connectionTimeout=300000
-Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
–Ditcamdc.dyncluster=true
```

   Al editar las entradas, tome nota de lo siguiente:

   - Todas las entradas deben estar en una sola línea.
   - Separe los distintos argumentos con espacios antes del signo `-`, no utilice espacios en ninguna otra parte.
   - Sustituya las siguientes variables por los nombres reales:
     - *$jvm-vendor*: el proveedor de la máquina virtual Java utilizado.
     - *$jvm-version*: la información de la versión de la JVM como, por ejemplo, 15 basado en Java 5, 16 basado en Java 6 o 17 basado en 7.
     - *$platform_Template_DCManualInput.txt*: el archivo `.txt` creado en el paso anterior.

     Ejemplo:

```
-agentlib:am_ibm_16=${WAS_SERVER_NAME}
-Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
-verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
aix64_Template_DCManualInput.txt
-Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
-Dsun.rmi.transport.connectionTimeout=300000
-Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
–Ditcamdc.dyncluster=true
```

9. Pulse **Aplicar**.
10. En el recuadro de diálogo Mensajes, pulse **Guardar**.
11. En el recuadro de diálogo Guardar en configuración maestra, realice los pasos siguientes:
    - Si está en un entorno de despliegue de red, asegúrese de que **Sincronizar cambios con nodos** está seleccionado y luego pulse **Guardar**.
    - Si no está en un entorno de despliegue de red, pulse **Guardar**.
12. Regrese para expandir **Clústeres**, ` pulse **Clústeres dinámicos** y pulse el mismo nombre de servidor.
13. En la pestaña **Configuración**, vaya a **Infraestructura de servidor** > **Java y gestión de procesos** > **Definición de procesos** > **Entradas de entorno**.
14. Dependiendo del sistema operativo, la plataforma de hardware y la JVM del servidor de aplicaciones, establezca la siguiente entrada de entorno:

Tabla 227. Entrada de entorno

Plataforma	Nombre de Entrada de entorno	Valor de Entrada de entorno
AIX R6.1 (JVM de 32 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix533:${ITCAMDCHOME}/toolkit/lib/aix533/ttapi
AIX R6.1 (JVM de 64 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix536:${ITCAMDCHOME}/toolkit/lib/aix536/ttapi
AIX R7.1 (JVM de 32 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix533:${ITCAMDCHOME}/toolkit/lib/aix533/ttapi
AIX R7.1 (JVM de 64 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix536:${ITCAMDCHOME}/toolkit/lib/aix536/ttapi
Linux x86_64 R2.6 (JVM de 64 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lx8266:${ITCAMDCHOME}/toolkit/lib/lx8266/ttapi
Linux Intel R2.6 (JVM de 32 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lx6263:${ITCAMDCHOME}/toolkit/lib/lx6263/ttapi
Linux ppc R2.6 (JVM de 32 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lpp263:${ITCAMDCHOME}/toolkit/lib/lpp263/ttapi
Linux ppc R2.6 (JVM de 64 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lpp266:${ITCAMDCHOME}/toolkit/lib/lpp266/ttapi
Windows (JVM de 32 bits)	PATH	/lib;${ITCAMDCHOME}/toolkit/lib/win32;${ITCAMDCHOME}/toolkit/lib/win32/ttapi
Windows (JVM de 64 bits)	PATH	/lib;${ITCAMDCHOME}/toolkit/lib/win64;${ITCAMDCHOME}/toolkit/lib/win64/ttapi

15. Establezca el nombre de entrada de entorno NLSPATH en el valor siguiente:

```
${ITCAMDCHOME}/toolkit/msg/%L/%N.cat
```

16. Pulse **Aceptar** y pulse **Guardar**.
17. En el recuadro de diálogo Guardar en configuración maestra, realice los pasos siguientes:

- Si está en un entorno de despliegue de red, asegúrese de que **Sincronizar cambios con nodos** está seleccionado y luego pulse **Guardar**.
- Si no está en un entorno de despliegue de red, pulse **Guardar**.

18. Regrese para expandir **Clústeres**, ` pulse **Clústeres dinámicos** y pulse el mismo nombre de servidor.
19. En la pestaña **Configuración**, vaya a **Infraestructura de servidor** > **Java y gestión de procesos** > **Definición de procesos** > **Máquina virtual Java** > **Propiedades adicionales: propiedades personalizadas**.
20. Pulse **Nuevo** para añadir los pares de nombre y valor siguientes y, a continuación, pulse **Aplicar**.
    - Cree una propiedad `am.home` y establezca su valor en el directorio siguiente:
      - Linux AIX *dir_instalación*`/yndchome/7.3.0.14.08/itcamdc`
      - Windows *dir_instalación*`\dchome\7.3.0.14.08\itcamdc`
    - Cree una propiedad `am.orig.wascell` y establezca su valor en el directorio de celda. Por ejemplo, `am.orig.wascell=cellname1`.
    - Cree una propiedad `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild` y establezca su valor en `true`.
    - Cree una propiedad `ITCAM_DC_ENABLED` y establezca su valor en `true`.
    - Cree una propiedad `TEMAGCCollector.gclog.path`. Si está establecido el argumento `verlogsegclog` de máquina virtual Java genérico, establezca el valor de la propiedad `TEMAGCCollector.gclog.path` en el mismo valor. De lo contrario, establezca la propiedad `TEMAGCCollector.gclog.path` en `None`.

      Consejo: Para identificar el valor de la propiedad `verlogsegclog`, en la pestaña **Configuración**, pulse **Infraestructura de servidor** > **Java y gestión de proceso** > **Definición de procesos** > **Máquina virtual Java**. El valor `verlogsegclog` se encuentra en el campo **Argumentos de JVM genéricos**.
21. En el recuadro de diálogo Mensajes, pulse **Guardar**.
22. En el recuadro de diálogo Guardar en configuración maestra, realice los pasos siguientes:
    - Si está en un entorno de despliegue de red, asegúrese de que **Sincronizar cambios con nodos** está seleccionado. Pulse **Guardar**.
    - Si no está en un entorno de despliegue de red, pulse **Guardar**.
23. En el panel de navegación, pulse **Entorno** > **Variables de WebSphere**.
24. Establezca las variables siguientes. Para cada variable, debe elegir el nivel de ámbito adecuado, en función del directorio de instalación del recopilador de datos en viarios sistemas. Si sistemas distintos tienen directorios de instalación distintos para el recopilador de datos, se deben establecer estas variables correctamente para cada ámbito de nivel de nodo. Si todos tienen el mismo directorio de instalación, el ámbito puede ser mayor, como en el nivel de clúster.
    - Establezca *ITCAMDCHOME* en el directorio siguiente:
      - Linux AIX *dir_instalación*`/yndchome/7.3.0.14.08/itcamdc`
      - Windows *dir_instalación*`\dchome\7.3.0.14.08\itcamdc`
    - Establezca *ITCAMDCVERSION* en la versión del recopilador de datos, por ejemplo, 7.3.0.14.08.
25. Pulse **Aceptar** y pulse **Guardar**.
26. En el recuadro de diálogo Guardar en configuración maestra, realice los pasos siguientes:
    - Si está en un entorno de despliegue de red, asegúrese de que **Sincronizar cambios con nodos** está seleccionado y luego pulse **Guardar**.
    - Si no está en un entorno de despliegue de red, pulse **Guardar**.

Después de modificarse la plantilla, los valores se sincronizan con todas las instancias de servidor del clúster dinámico. Los servidores nuevos creados dinámicamente tendrán también los mismos parámetros de configuración del recopilador de datos.

27. Reinicie la instancia de servidor de aplicaciones para que se active el recopilador de datos. El recopilador de datos lee los archivos de valores y crea el directorio de tiempo de ejecución.

Opcional: mostrar el nombre de la JVM real para distinguir los miembros del clúster

Acerca de esta tarea

En la Consola de Cloud APM, el nombre de instancia de Agente de WebSphere Applications toma el formato *nombre_host:*:*nombre_servidor_was*:KYNS y tiene una longitud máxima de 32 caracteres. En el entorno de clúster dinámico, los nombres de miembro de clúster dinámico se utilizan para el calificador medio *nombre_servidor_was*.

A veces, los nombres de miembro de clúster están truncados debido al límite de longitud de caracteres. En este caso, puede especificar el nombre de la JVM real que se utilizará para el calificador medio en el nombre de la instancia de agente.

Procedimiento

Realice los pasos siguientes para mostrar el nombre de la JVM real en el nombre de la instancia de agente:

1. Inicie la sesión en la consola administrativa de WebSphere para actualizar los argumentos de JVM genéricos añadiendo una nueva variable de entorno *${MEP_NAME}* como se indica a continuación:

```
-agentlib:am_$jvm-vendor_$jvm-version=${MEP_NAME}${WAS_SERVER_NAME}
-Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
-verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
$platform_Template_DCManualInput.txt
-Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
-Dsun.rmi.transport.connectionTimeout=300000
-Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
–Ditcamdc.dyncluster=true
```

   Ejemplo:

```
-agentlib:am_ibm_16=${MEP_NAME}${WAS_SERVER_NAME}
-Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
-verbosegc
-Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
aix64_Template_DCManualInput.txt
-Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
-Dsun.rmi.transport.connectionTimeout=300000
-Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
–Ditcamdc.dyncluster=true
```

2. Guarde y aplique los cambios.
3. En el panel de navegación, pulse **Entorno** > **Variables de WebSphere** para definir la variable *${MEP_NAME}* para cada miembro de clúster dinámico. Establezca el valor en el nombre de la JVM real del miembro de clúster.
4. Guarde y aplique los cambios.
5. Reinicie la instancia del servidor de aplicaciones.

   En la Consola de Cloud APM, se muestra una nueva instancia de Agente de WebSphere Applications cuyo nombre contiene el valor *${MEP_NAME}* que acaba de especificar.

Configuración dinámica de la recopilación de datos en la página Configuración de agente

Después de habilitar el soporte para el rastreo de transacciones o la recopilación de datos de diagnóstico en el recopilador de datos, utilice la página **Configuración de agente** para habilitar o inhabilitar dinámicamente la recopilación de datos.

Antes de empezar

- Debe instalar y configurar el Monitoring Agent for WebSphere Applications.
- Para habilitar o inhabilitar el rastreo de transacciones para los servidores de aplicaciones supervisados, debe instalar el Rastreo de transacciones. También de habilitar el soporte para el rastreo de transacciones en el agente tal como se describe en "Configuración interactiva del recopilador de datos" en la página 870. Si sigue el procedimiento sencillo de configuración, el recopilador de datos se configurará de manera automática con soporte para el rastreo de transacciones.
- Para habilitar o inhabilitar el rastreo de datos de diagnóstico, incluyendo el rastreo de métodos, debe tener Cloud APM, Advanced. También debe habilitar el soporte para la recopilación de información de diagnóstico y de rastreo de métodos en el recopilador de datos, tal como se describe en "Configuración interactiva del recopilador de datos" en la página 870. (No disponible para Cloud APM, Base).

Consejo: La página **Configuración del agente** visualiza todos los servidores que están supervisados por el agente. Si falta algún servidor, es posible que no se supervise correctamente. Compruebe los archivos de registro del agente en el sistema supervisado para ver si hay mensajes de error, por ejemplo, errores de conexión.

Recuerde: El Agente de WebSphere Applications solamente admite Db2 y Oracle como origen de datos. Para otros tipos de orígenes de datos, algunos valores de ICR podrían parecer nulos en los paneles de instrumentos y los widgets del grupo del rastreo de transacciones.

Procedimiento

Complete los pasos siguientes para configurar la colección de datos para cada servidor:

1. En la barra de navegación, pulse **Configuración del sistema** > **Configuración del agente**.
   Se mostrará la página **Configuración del agente**.
2. Pulse el separador **Aplicaciones WebSphere**.
3. Marque los recuadros de selección de los servidores en los que desea supervisar la recopilación de datos y lleve a cabo una de las acciones siguientes de la lista **Acciones**:
   - Para habilitar el rastreo de transacciones, pulse **Habilitar rastreo de transacciones**. El estado de la columna **Rastreo de transacciones actual** se actualizará a Sí para cada servidor seleccionado.
   - Para habilitar solo la recopilación de datos de diagnóstico, pulse **Habilitar modalidad de diagnóstico**. El estado de la columna **Modalidad de diagnóstico actual** se actualizará a Sí para cada servidor seleccionado.
   - Para recopilar tanto los datos de diagnóstico como la información de rastreo de método, pulse **Habilitar modalidad de diagnóstico y rastreo de método**. El estado de las columnas **Modalidad de diagnóstico actual** y **Rastreo de método actual** se actualiza a Sí para cada servidor seleccionado.
   - Para inhabilitar el rastreo de transacciones para el servidor seleccionado, pulse **Inhabilitar rastreo de transacciones**. El estado de la columna **Rastreo de transacciones actual** se actualizará a No para cada servidor seleccionado.
   - Si para el servidor seleccionado solo está habilitada la recopilación de datos de diagnóstico, para inhabilitar la recopilación de datos, pulse **Inhabilitar modalidad de diagnóstico**. El estado de la columna **Modalidad de diagnóstico actual** se actualizará a No para cada servidor seleccionado.
   - Si los datos de diagnóstico y los datos de rastreo de método están habilitados para el servidor seleccionado, para inhabilitar la recopilación de datos, pulse **Inhabilitar modalidad de diagnóstico y rastreo de método**. El estado de las columnas **Modalidad de diagnóstico actual** y **Rastreo de método actual** se actualiza a No para cada servidor seleccionado.

   Recuerde:

   - a menos que se configure el soporte para el rastreo de transacciones o la recopilación de datos de diagnóstico en el recopilador de datos, las operaciones de la página **Configuración de agente** no permite la recopilación de datos y el valor de la columna se establece en No.

- Si el perfil de servidor de aplicación se ha configurado para utilizar `127.0.0.1` como nombre de host, la columna **Dirección IP** en la página **Configuración de agente** muestra la dirección IP del host donde Agente de WebSphere Applications está instalado y en ejecución.

Resultados
Ha configurado la recopilación de datos para cada servidor seleccionado. Los datos del rastreo de transacciones y los datos de diagnóstico se pueden visualizar en los paneles de instrumentos de topología, tras habilitar la colección de datos.

Importante: Si se reinicia un servidor de aplicaciones, quizá tenga que volver a habilitar el rastreo de transacciones o la recopilación de datos de diagnóstico para el servidor.

Habilitación de la supervisión de fugas de memoria
Para que el panel de instrumentos Análisis de memoria contenga datos, debe habilitar la supervisión de fugas de memoria para el recopilador de datos. Si el JRE utilizado por el servidor de aplicaciones está soportado, la función de supervisión de fugas de memoria se habilitará de forma predeterminada después de habilitar la recopilación de datos de diagnóstico.

Antes de empezar

- Asegúrese de que `-Xtrace:none` no está definido en los argumentos de JVM para el servidor de aplicaciones.
- Cuando la supervisión de fugas de memoria está habilitada, los valores siguientes están definidos en los argumentos de JVM para el servidor de aplicaciones. Si ha definido estos valores en sus argumentos de JVM actuales, asegúrese de que no haya ningún problema en el hecho de que la configuración del recopilador de datos los cambie.

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
```

- Asegúrese de que el JRE utilizado por el servidor de aplicaciones es de una de las siguientes versiones:
  - IBM JRE 1.6.0 SR16 FP3 o posterior
  - IBM JRE 1.6.1 SR8 FP3 o posterior
  - IBM JRE 1.7.0 SR8 FP10 o posterior
  - IBM JRE 1.7.1 SR2 FP10 o posterior
  - IBM JRE 1.8 o posterior
  - Otros JRE de IBM JRE posteriores a 1.6.0 SR7 con iFix para el APAR IV67574

Acerca de esta tarea

La función de supervisión de fugas de memoria requiere el componente IBM Health Center de IBM JRE. Asegúrese de que el JRE utilizado por el servidor de aplicaciones esté soportado por esta función.

- En sistemas AIX o Linux, al configurar el recopilador de datos para habilitar la recopilación de datos de diagnóstico, si el JRE actual está soportado, el programa de utilidad de configuración comprueba automáticamente si el componente Health Center es elegible y lo actualiza si no lo es.
- En sistemas Windows, debe actualizar manualmente el componente Health Center si la versión actual no está soportada, ya que el programa de utilidad de configuración no puede sustituir archivos de un JRE en ejecución.

Recuerde: el procedimiento siguiente sólo es necesario en sistemas Windows. En sistemas AIX o Linux, para habilitar la supervisión de fugas de memoria, sólo necesita asegurarse de que la versión de JRE está soportada y la recopilación de datos de diagnóstico esté habilitada. En sistemas Solaris, Health Center de IBM JRE no está soportado, por lo que la supervisión de fugas de memoria no puede habilitarse en sistemas Solaris.

Procedimiento

1. Compruebe la versión de IBM Health Center que se incluye en el JRE utilizado por el servidor de aplicaciones.
   a) En el indicador de mandatos, vaya al directorio `bin` del directorio inicial de JRE.
   b) Escriba `java -Xhealthcenter -version` y pulse Intro.

   El mandato devolverá la versión de JRE y la versión de IBM Health Center. La función de supervisión de fugas de memoria requiere IBM Health Center 3.0.11 o posterior.
2. Si la versión de IBM Health Center no es elegible, actualice el JRE a una versión que contenga IBM Health Center 3.0.11 o posterior.
3. Ejecute el programa de utilidad de configuración o reconfiguración del recopilador de datos para habilitar la recopilación de datos de diagnóstico.
   - Si no ha configurado el recopilador de datos, utilice el programa de utilidad `simpleconfig` o `config`.
   - Si ha configurado el recopilador de datos, utilice el programa de utilidad `simpleconfig`.

   Recuerde: si ha habilitado la recopilación de datos de diagnóstico antes de actualizar el JRE, sigue siendo necesario volver a ejecutar el programa de utilidad de configuración de la recopilación de datos.

Configuración de PMI

Para visualizar datos de rendimiento en los paneles de instrumentos de supervisión operativos, Performance Monitoring Infrastructure (PMI) en el WebSphere Application Server debe estar configurada para recopilar datos de rendimiento.

Acerca de esta tarea

Utilice la consola de administración de WebSphere para habilitar la PMI y establecer el nivel de PMI en WebSphere Application Server.

PMI proporciona cuatro niveles predefinidos:

1. Ninguno
2. Basic
3. Ampliado
4. Todos

Puede utilizar una opción personalizada para habilitar e inhabilitar de forma selectiva estadísticas individuales. Cada nivel incluye las estadísticas desde el nivel inferior.

Para visualizar datos en los paneles de instrumentos de supervisión operativos, los atributos que se utilizan en los cálculos del panel deben incluirse en el nivel seleccionado.

De forma predeterminada, el Agente de WebSphere Applications establece el nivel de PMI lo suficientemente elevado para recopilar los atributos requeridos.

Restricción: Para ver datos en algunos de los widgets de grupo Process Server y Transaction Manager, debe establecer manualmente el nivel de PMI. Para obtener más información, consulte la ayuda contextual de los widgets de grupo.

Si modifica el nivel de PMI a través de la consola administrativa de WebSphere, debe verificar que el nivel es lo suficientemente elevado para recopilar los datos requeridos.

Procedimiento

- Para habilitar PMI en el servidor de aplicaciones, siga estos pasos:
  a) En la consola de administración WebSphere, expanda **Supervisión y ajuste** y, a continuación, seleccione **Performance Monitoring Infrastructure (PMI)**.
  b) En la lista de servidores, pulse el nombre de su servidor.

c) Pulse la pestaña Configuración y marque el recuadro de selección **Habilitar Performance Monitoring Infrastructure (PMI)**.

d) Pulse **Aplicar** o **Aceptar**.

e) Pulse **Guardar** para habilitar PMI.

- Para establecer el nivel de PMI en el servidor de aplicaciones, siga estos pasos:

  a) En la consola de administración WebSphere, expanda **Supervisión y ajuste** y, a continuación, seleccione **Performance Monitoring Infrastructure (PMI)**.

  b) En la lista de servidores, pulse el nombre de su servidor.

  c) Pulse la pestaña Configuración y seleccione el conjunto de estadísticas a utilizar: Básico, Ampliado, Todo o Personalizado.

  d) Pulse **Aplicar** o **Aceptar**.

  e) Pulse **Guardar** para establecer el nivel de PMI

  Si desea más información sobre el nivel de PMI que es necesario para cada atributo, consulte la sección "Dashboard attributes" de la Referencia de Agente de WebSphere Applications. Se muestra la sobrecarga de supervisión que se produce cuando se activa la recopilación de cada atributo.

Restauración de la configuración del servidor de aplicaciones a partir de una copia de seguridad
Si ha configurado una instancia de servidor de aplicaciones autónomo para la recopilación de datos ya sea manualmente o con el programa de utilidad de configuración o migración, y el servidor de aplicaciones no se inicia, debe restaurar la configuración del servidor de aplicaciones a partir de una copia de seguridad. Si no ha creado ninguna copia de seguridad, póngase en contacto con el personal de soporte de IBM.

Acerca de esta tarea

En un entorno de despliegue de red, si ha configurado una instancia de servidor de aplicaciones para la recopilación de datos, ya sea manualmente o mediante el programa de utilidad de configuración o migración, y el servidor de aplicaciones no se inicia, tiene estas opciones:

- Puede restaurar la configuración del servidor de aplicaciones a partir de una configuración de copia de seguridad. Si no ha creado ninguna copia de seguridad, póngase en contacto con el personal de soporte de IBM.
- Puede desconfigurar manualmente el recopilador de datos. El gestor de despliegue y el agente de nodo en el servidor de aplicaciones deben estar en ejecución. Para obtener más información, consulte “Eliminación manual de la configuración del recopilador de datos de una instancia del servidor de aplicaciones” en la página 157.

Esta sección solamente se aplica a los sistemas operativos Windows, UNIX y Linux.

Procedimiento

Para aplicar la configuración de copia de seguridad utilizando el mandato **restoreConfig**, utilice uno de los siguientes procedimientos:

- En un entorno que no es de despliegue de red, realice los siguientes pasos:

  a) Localice el archivo de configuración de copia de seguridad.

  El directorio predeterminado es *dir_inicio_dc*/data. Si hay varios archivos de copia de seguridad, compruebe la fecha y hora de modificación del archivo. Debe ser la fecha y hora de la configuración anómala. Si no ha completado ninguna otra configuración del recopilador de datos en el mismo host después de la anómala, utilice el archivo más reciente del directorio.

  b) Detenga todas las instancias del servidor de aplicaciones.

  c) Ejecute el mandato **restoreConfig** desde el directorio *dir_inicio_servidor_aplic*/profiles/*nombre_perfil*/bin.

  La sintaxis del mandato es la siguiente:

  – Windows `restoreConfig.bat` *vía_acceso_completa_a_archivo_copia_seguridad*

– Linux AIX `./restoreConfig.sh` *vía_acceso_completa_a_archivo_copia_seguridad*

Para más información sobre los argumentos del mandato **restoreConfig**, consulte WebSphere Application Server Knowledge Center.

d) Inicie de nuevo las instancias del servidor de aplicaciones.

- En un entorno de despliegue de red, siga estos pasos:

a) Localice el archivo de configuración de copia de seguridad.

El directorio predeterminado es *dir_inicio_dc*/data. Si hay varios archivos de copia de seguridad, compruebe la fecha y hora de modificación del archivo; debe ser la fecha y hora de la configuración anómala. Si no ha completado ninguna otra configuración del recopilador de datos en el mismo host después de la anómala, utilice el archivo más reciente del directorio.

b) Detenga todas las instancias del servidor de aplicaciones.

c) Cree un directorio temporal en la vía de acceso que le interese (*directorio_temp*). En un sistema UNIX o Linux, créelo en el directorio /tmp.

d) Ejecute el mandato restoreConfig desde el directorio *dir_inicio_servidor_aplic*/profiles/*nombre_perfil*/bin.

La sintaxis del mandato es la siguiente:

– Windows `restoreConfig.bat` *vía_acceso_completa_a_archivo_copia_seguridad*

– Linux AIX `./restoreConfig.sh` *vía_acceso_completa_a_archivo_copia_seguridad*

El mandato **restoreConfig** restaura el servidor de aplicaciones original en el directorio temporal.

e) Copie los archivo server.xml, variables.xml y pmi-config.xml del directorio temporal en el sistema de Deployment Manager.

– Directorio de origen: *directorio_temp*/*inicio_configuración_restaurada*/cells/*nombre_célula*/nodes/*nombre_nodo*/servers/*nombre_servidor*

– Directorio de destino: *dir_inicio_servidor_aplic*/profiles/*nombre_perfil*/config/cells/*nombre_célula*/nodes/*nombre_nodo*/servers/*nombre_servidor*

f) Realice una sincronización de nodos desde la consola de administración del gestor de despliegue para el nodo.

g) En la consola de administración del gestor de despliegue, guarde los cambios realizados en la configuración maestra.

h) Inicie las instancias del servidor de aplicaciones.

Configuración del recopilador de datos para aplicaciones locales

Para supervisar el perfil de Liberty en Linux para System x, puede desplegar directamente un recopilador de datos autónomo en el directorio de Liberty local sin instalar el Agente de WebSphere Applications.

Antes de empezar

1. Descargue el paquete de recopilador de datos IBM_Data_Collectors_Install.tgz del sitio web de IBM Passport Advantage. Para obtener instrucciones detalladas, consulte el sitio web de “Descarga de los agentes y recopiladores de datos” en la página 107.
2. Si las reglas de cortafuegos no permiten establecer conexiones HTTPS transparentes de salida a host externos, puede configurar recopiladores de datos para enviar el tráfico a un proxy directo. Para obtener instrucciones, consulte “Configuración de recopiladores de datos para la comunicación mediante un proxy directo” en la página 169.
3. El recopilador de datos necesita la característica monitor-1.0. Puede descargar esta característica desde el repositorio de características de Liberty con el mandato **installUtility**. Para obtener

instrucciones, consulte la sección sobre la descarga de activos en el Knowledge Center de WebSphere Application Server Network Deployment.

4. Para que el panel de instrumentos Análisis de memoria contenga datos, debe habilitar la recopilación de asignación de memoria para el recopilador de datos durante la configuración. Esta característica de diagnóstico necesita IBM Health Center 3.0.8 o posterior. Si no se pude elegir la versión de IBM Health Center, actualice el JRE utilizado por el servidor de aplicaciones a una versión que contenga IBM Health Center 3.0.8 o una versión posterior.

   Consejo: Para comprobar la versión de IBM Health Center incluida en el JRE utilizado por el servidor de aplicaciones, sitúese en el directorio `bin` dentro del directorio de inicio de JRE y emita el mandato `java -Xhealthcenter -version`.

Acerca de esta tarea

Puede optar por configurar manualmente el recopilador de datos o utilizar el script de configuración proporcionado para configurarlo.

Procedimiento

- Para configurar manualmente el recopilador de datos, obtenga los archivos del recopilador de datos del paquete del recopilador de datos y a continuación modifique algunos archivos locales para el servidor Liberty.
  a) Ejecute el mandato siguiente para extraer archivos del paquete recopilador de datos.

  ```
  tar -xzf IBM_Data_Collectors_Install.tgz
  ```

  El paquete `liberty_datacollector_8.1.4.0.tgz` está incluido en el directorio extraído.

  b) Extraiga los archivos del paquete `liberty_datacollector_8.1.4.0.tgz` en un directorio local con el mandato siguiente. El directorio extraído se convertirá en el directorio inicial del recopilador de datos.

  ```
  tar -xzf liberty_datacollector_8.1.4.0.tgz
  ```

  Por ejemplo, para extraer los archivos en el directorio `/opt/ibm/apm/`, emita los mandatos siguientes:

  ```
  cd /opt/ibm/apm
  tar -xzf liberty_datacollector_8.1.4.0.tgz
  ```

  Encontrará los archivos extraídos en el directorio `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`. Este directorio es el directorio de inicio del recopilador de datos (*inicio_dc*) en los pasos siguientes.

  c) Vaya al directorio inicial del servidor Liberty. Por ejemplo, `/opt/ibm/wlp/usr/servers/defaultServer`.

  d) Edite el archivo `jvm.options` añadiendo los parámetros siguientes. Si el archivo `jvm.options` no existe, créelo con un editor de texto.

  ```
  -agentlib:am_ibm_16=nombre_servidor
  -Xbootclasspath/p:inicio_dc/toolkit/lib/bcm-bootstrap.jar
  -Djava.security.policy=inicio_dc/itcamdc/etc/datacollector.policy
  -Dliberty.home=inicio_liberty
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  -verbosegc
  -Xverbosegclog:vía_acceso_absoluta_archivo_registro,1,10000
  ```

  Al añadir las entradas, tenga en cuenta lo siguiente:

  – Cada entrada debe estar en una sola línea.
  – Sustituya *nombre_servidor* por el nombre del servidor Liberty.

- Sustituya *inicio_dc* por el directorio de inicio del recopilador de datos. Por ejemplo `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`.
- Sustituya *inicio_liberty* por el directorio raíz de instalación de Liberty. Por ejemplo, `/opt/ibm/wlp`.
- Si el servidor Liberty está soportando mucha carga de trabajo, añada el parámetro `-Xmx` para asignar un tamaño de almacenamiento adicional de 512M al recopilador de datos. Por ejemplo, `-Xmx1024M`.
- Las líneas `-Xhealthcenter:level=inprocess` y `-Xgc:allocationSamplingGranularity=10000` son opcionales. Añada las dos líneas solo si desea habilitar la recopilación de la asignación de memoria, que está inhabilitada de forma predeterminada. La habilitación de la recopilación de asignación de memoria es necesaria para que el panel de instrumentos de Análisis de memoria contenga datos.
- La línea `-Xverbosegclog:`*`vía_acceso_absoluta_archivo_registro`*`,1,10000` es opcional y especifica la vía de acceso al archivo de registro de recopilación de recogida de basura. Si no se especifica, los registros se escriben en un archivo y rotan cada 10000 anomalías de asignación. El archivo `stdout` o `stderr` original (`console.log`) puede ser muy grande cuando se ejecuta el servidor. Añada esta línea si desea guardar los archivos de registro de salida de recogida de basura en otro directorio y limitar el numero y el tamaño de los archivos de registro. Si la vía de acceso especificada no es válida, esta línea no surte efecto y el archivo de registro de recogida de basura permanece en el archivo `stdout` o `stderr`.

e) Abra el archivo `server.env` en el mismo directorio y añada la vía de acceso siguiente a la entrada de entorno. Si el archivo `server.env` no existe, créelo con un editor de texto.

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/lib:inicio_dc/toolkit/lib/lx8266:inicio_dc/
toolkit/lib/lx8266/ttapi
```

Al añadir las entradas, tenga en cuenta lo siguiente:

- Cada entrada debe estar en una sola línea.
- Sustituya *inicio_dc* por el directorio de inicio del recopilador de datos. Por ejemplo `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`.

f) Modifique `server.xml` en el mismo directorio para habilitar la característica de supervisión añadiendo la línea siguiente a la sección `<featureManager>`:

```
<feature>monitor-1.0</feature>
```

g) Reinicie el servidor Liberty.

- Para configurar el recopilador de datos respondiendo a solicitudes, utilice el script de configuración que se proporciona en los paquetes de recopilador de datos.

a) Ejecute el mandato siguiente para extraer archivos del paquete recopilador de datos.

```
tar -xzf IBM_Data_Collectors_Install.tgz
```

El paquete `liberty_datacollector_8.1.4.0.tgz` está incluido en el directorio extraído.

b) Extraiga los archivos del paquete `liberty_datacollector_8.1.4.0.tgz` con el mandato siguiente.

```
tar -xzf liberty_datacollector_8.1.4.0.tgz
```

Por ejemplo,

```
cd /opt/ibm
tar -xzf liberty_datacollector_8.1.4.0.tgz
```

Los archivos del recopilador de datos extraídos están en el directorio `liberty_dc`.

c) Vaya al directorio `liberty_dc/.gdc/7.3.0.14.08/bin` e inicie el script de configuración ejecutando el mandato siguiente:

```
./config_liberty_dc.sh
```

d) Cuando se le solicite, especifique la raíz de su directorio de instalación de Liberty o acepte el valor predeterminado. Por ejemplo, `/opt/ibm/wlp`.

e) Cuando se le solicite, especifique el inicio de la máquina virtual Java utilizada por el servidor de aplicaciones o acepte el valor predeterminado. Por ejemplo, `/opt/ibm/java`.

f) El programa de configuración puede descubrir automáticamente y listar los servidores de aplicaciones que no están configurados en el directorio especificado. Especifique el número que corresponde al servidor Liberty que desea configurar. Para seleccionar más de un servidor, separe los números mediante espacios o especifique * para seleccionarlos todos.

g) Cuando el programa de configuración termine de actualizar archivos para todos los servidores de Liberty, actualice manualmente el tamaño de almacenamiento dinámico de la máquina virtual Java para asignar un almacenamiento dinámico adicional de 512M al recopilador de datos.

h) Reinicie los servidores para que la configuración surta efecto.

Resultados

El recopilador de datos se ha configurado y está conectado al Servidor de Cloud APM. La supervisión de recursos el rastreo de transacción y los datos de diagnóstico están habilitados. Sin embargo, la recopilación de almacenamiento dinámico y la recopilación de asignación de memoria están inhabilitadas. Puede habilitarlas con los archivos de propiedades del recopilador de datos si necesita los datos en los paneles de instrumentos Vuelco de almacenamiento dinámico y Análisis de memoria.

Qué hacer a continuación

- Para ver los datos de supervisión de los servidores Liberty, inicie la Consola de Cloud APM. Para obtener instrucciones, consulte Inicio de la consola de Cloud APM. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte Gestión de aplicaciones.

  Recuerde: Cuando añada la instancia de recopilador de datos de Liberty en Panel de instrumentos de aplicaciones, seleccione **Liberty Runtime** en lugar de **WebSphere Application Server** en la lista de componentes.
- Para que el panel de instrumentos Vuelco de almacenamiento dinámico y/o Análisis de memoria, necesita habilitar el recopilador de datos para la recopilación de instantáneas de almacenamiento dinámico y/o la recopilación de asignación de memoria, lo que se puede hacer en los archivos `.properties` del recopilador de datos. Consulte “Habilitación o inhabilitación del rastreo de transacciones y la recopilación de datos de diagnóstico” en la página 925.
- Si el archivo de claves o el Servidor de Cloud APM cambian, vuelva a conectar el recopilador de datos al Servidor de Cloud APM. Para obtener instrucciones, consulte “Reconexión del recopilador de datos al Servidor de Cloud APM” en la página 193.

Desconfigurar el recopilado de datos para aplicaciones locales

Si no necesita supervisar los servidores Liberty o si desea actualizar el recopilador de datos a una versión nueva, debe desconfigurar el recopilador de datos que ha desplegado en el servidor Liberty.

Acerca de esta tarea

Para desconfigurar el recopilador de datos desplegado en el servidor Liberty, retrotraiga los cambios realizados al configurar el recopilador de datos. Puede optar por configurar el recopilador de datos manualmente o con el script `unconfig_liberty_dc` proporcionado.

Procedimiento

- Para desconfigurar manualmente el recopilador de datos, siga estos pasos:

  a) Vaya al directorio inicial del servidor Liberty. Por ejemplo, `/opt/ibm/wlp/usr/servers/defaultServer`.

  b) Edite el archivo `jvm.options` para eliminar los parámetros siguientes si existen.

```
-agentlib:am_ibm_16=nombre_servidor
-Xbootclasspath/p:inicio_dc/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=inicio_dc/itcamdc/etc/datacollector.policy
-Dliberty.home=inicio_liberty
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
-verbosegc
-Xverbosegclog:vía_acceso_absoluta_archivo_registro,1,10000
```

c) Edite el archivo `server.env` en el mismo directorio para eliminar el valor siguiente para **LD_LIBRARY_PATH**

```
/lib:inicio_dc/toolkit/lib/lx8266:inicio_dc/toolkit/lib/lx8266/ttapi
```

donde *inicio_dc* es el directorio de inicio del recopilador de datos. Por ejemplo `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`.

d) Edite el archivo `server.xml` en el mismo directorio para eliminar `<feature>monitor-1.0</feature>` de la sección `<featureManager>`.

e) Reinicie el servidor Liberty.

- Para desconfigurar el recopilador de datos con el script `unconfig_liberty_dc.sh`, siga estos pasos:

a) Vaya al directorio *inicio_dc*`/bin`. Por ejemplo `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08/bin`.

b) Inicie el script de desconfiguración ejecutando el mandato siguiente:

```
./unconfig_liberty_dc.sh
```

c) Cuando se le solicite, especifique la raíz de su directorio de instalación de Liberty o acepte el valor predeterminado. Por ejemplo, `/opt/ibm/wlp`.

d) El programa de desconfiguración puede descubrir automáticamente y listar los servidores de aplicaciones que están configurados en el directorio especificado. Especifique el número que corresponde al servidor Liberty que desea desconfigurar. Para seleccionar más de un servidor, separe los números mediante espacios o especifique * para seleccionarlos todos.

e) Cuando el programa de desconfiguración termine de actualizar archivos para todos los servidores de Liberty, reinicie los servidores para que los cambios surtan efecto.

Qué hacer a continuación

Tras desconfigurar el recopilador de datos, la Consola de Cloud APM continúa mostrando el recopilador de datos en cualquier aplicación a la que haya añadido el recopilador de datos. La Consola de Cloud APM mostrará que no hay datos disponibles para la aplicación y no indicará que el recopilador de datos está fuera de línea. Para obtener información sobre cómo eliminar el recopilador de datos de aplicaciones y de grupos de recursos, consulte “Eliminación de recopiladores de datos de Consola de Cloud APM” en la página 196.

También puede suprimir el directorio de inicio del recopilador de datos si ya no lo necesita.

Configuración del recopilador de datos de Liberty para aplicaciones IBM Cloud

Para supervisar un perfil de Liberty que se esté ejecutando en el entorno IBM Cloud , debe descargar el paquete de recopilador de datos de de IBM Marketplace, desplegar el recopilador de datos en sus archivos de aplicación local y a continuación enviar las actualizaciones a IBM Cloud.

Antes de empezar

Se da por supuesto que la aplicación Liberty se envía al entorno IBM Cloud mediante los mandatos de Cloud Foundry. El archivo `manifest.yml` y el directorio de inicio del servidor Liberty (que contiene el archivo `server.xml`) ya existen.

Si la aplicación Liberty se despliega como archivo WAR, debe modificar algunos archivos locales para actualizar la aplicación enviando un directorio local que contenga el archivo WAR y los archivos de recopilador de datos. Aquí se proporcionan un ejemplo para explicar cómo obtener un directorio de inicio de servidor Liberty local si sólo se tiene un archivo WAR.

1. Emita el mandato siguiente para ejecutar la aplicación Liberty localmente:

   ```
   mvn install liberty:run-server
   ```

   En el directorio que contiene el archivo WAR de Liberty, se crea un subdirectorio, `/liberty/wlp/usr/servers/defaultServer`. Este directorio puede actuar como el directorio inicial del servidor Liberty en el procedimiento siguiente.
2. Desde el directorio raíz que contiene el archivo WAR de Liberty, copie toda la carpeta *nombre_aplicación*-SNAPSHOT en el directorio `/liberty/wlp/usr/servers/defaultServer`.
3. En el directorio `/liberty/wlp/usr/servers/defaultServer`, edite el archivo `bootstrap.properties` para modificar la vía de acceso de **appLocation**. La vía de acceso de **appLocation** debe establecerse en la vía de acceso relativa al directorio de aplicación en IBM Cloud.
4. Elimine las carpetas `logs` y `workarea`. No es necesario enviarlas a IBM Cloud.
5. Modifique el valor **path** en el archivo `manifest.yml` para que apunte al directorio `defaultServer`.

   Por ejemplo, `path: target/liberty/wlp/usr/servers/defaultServer`.

Procedimiento

Siga estos pasos para configurar el recopilador de datos de Liberty:

1. Descargue el paquete de recopilador de datos denominado `IBM_Data_Collectors_Install.tgz`de IBM Marketplace. Para obtener instrucciones detalladas, consulte “Descarga de los agentes y recopiladores de datos” en la página 107.
2. Ejecute el mandato siguiente para extraer archivos del paquete recopilador de datos.

   ```
   tar -xzf IBM_Data_Collectors_Install.tgz
   ```

   El paquete `liberty_datacollector_8.1.4.0.tgz` está incluido en el directorio extraído.
3. Extraiga los archivos del paquete `liberty_datacollector_8.1.4.0.tgz` en un directorio temporal.

   ```
   tar -xzf liberty_datacollector_8.1.4.0.tgz
   ```

   Por ejemplo,

   ```
   cd /root/tmp
   tar -xzf liberty_datacollector_8.1.4.0.tgz
   ```

   Encontrará los archivos extraídos en el directorio `liberty_dc` dentro del directorio temporal.
4. Copie el directorio `.gdc` del directorio `liberty_dc` en el directorio inicial del servidor Liberty en el que está almacenado el archivo `server.xml`. El directorio inicial del servidor Liberty se indica como *inicio_servidor_liberty* en los pasos siguientes.

   ```
   cp -rf dir_temp/liberty_dc/.gdc inicio_servidor_liberty
   ```

   Por ejemplo,

   ```
   cp -rf /root/tmp/liberty_dc/.gdc /opt/liberty855/wlp/usr/servers/defaultServer/
   ```
5. Copie o fusione el contenido de los archivos `jvm.options` y `server.env` del directorio `liberty_dc/etc` en el directorio *inicio_servidor_liberty*.

- Si los archivos `jvm.options` y `server.env` no existen en el directorio *`inicio_servidor_liberty`*, copie los dos archivos de *`dir_temp`*`/liberty_dc/etc` en *`inicio_servidor_liberty`*.

  ```
  cp dir_temp/liberty_dc/etc/jvm.option inicio_servidor_liberty
  cp dir_temp/liberty_dc/etc/server.env inicio_servidor_liberty
  ```

- Si el archivo `jvm.options` o `server.env` existe en el directorio *`inicio_servidor_liberty`*, fusione el contenido con los del directorio *`dir_temp`*`/liberty_dc/etc`.

6. Si las aplicaciones IBM Cloud no pueden conectar directamente con el Servidor de Cloud APM debido a los valores de red o de cortafuegos, configure el recopilador de datos para enviar tráfico de datos a través de un proxy de reenvío. Para hacerlo, edite el archivo `jvm.options` de una de las maneras siguientes:

   - Si la autenticación no es necesaria, añada las líneas siguientes al archivo:

     ```
     -Dhttp.proxyHost=host_proxy_http
     -Dhttp.proxyPort=puerto_proxy_http
     -Dhttps.proxyHost=host_proxy_http
     -Dhttps.proxyPort=puerto_proxy_http
     -Djava.net.useSystemProxies=true
     ```

   - Si se necesitan un nombre de usuario y una contraseña para acceder al servidor de proxy directo, añada las líneas siguientes al archivo:

     ```
     -Dhttp.proxyHost=host_proxy_http
     -Dhttp.proxyPort=puerto_proxy_http
     -Dhttp.proxyUser=usuario_proxy_http
     -Dhttp.proxyPassword=contraseña_proxy_http
     -Dhttps.proxyHost=host_proxy_http
     -Dhttps.proxyPort=puerto_proxy_http
     -Dhttps.proxyUser=usuario_proxy_http
     -Dhttps.proxyPassword=contraseña_proxy_http
     -Djava.net.useSystemProxies=true
     ```

7. Modifique el archivo `server.xml` dentro del directorio de inicio del servidor Liberty para habilitar la característica de supervisión añadiendo la línea siguiente a la sección `<featureManager>`:

   ```
   <featureManager>
                <feature>monitor-1.0</feature>
   </featureManager>
   ```

8. Modifique el archivo `manifest.yml` de la aplicación Liberty para asignar memoria 512M adicional.
9. Abra un indicador de mandatos, sitúese en el directorio local que contiene el archivo `manifest.yml` del servidor Liberty. Por ejemplo `/opt/liberty855/`.
10. Inicie la sesión en IBM Cloud y actualice el perfil de Liberty con el mandato **`cf push`**.

Resultados

El recopilador de datos se ha configurado y está conectado al Servidor de Cloud APM. La supervisión de recursos el rastreo de transacción y los datos de diagnóstico están habilitados. Sin embargo, la recopilación de almacenamiento dinámico y la recopilación de asignación de memoria están inhabilitadas. Puede habilitarlas con los archivos de propiedades del recopilador de datos si necesita los datos en los paneles de instrumentos Vuelco de almacenamiento dinámico y Análisis de memoria.

Qué hacer a continuación

- Para ver los datos de supervisión de la aplicación IBM Cloud, inicie la Consola de Cloud APM. Para obtener instrucciones, consulte Inicio de la consola de Cloud APM. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte Gestión de aplicaciones.

  Recuerde: Cuando desee añadir la instancia de recopilador de datos de Liberty en Panel de instrumentos de aplicaciones, seleccione **Liberty Runtime** en lugar de **WebSphere Application Server** en la lista de componentes.

- Para que el panel de instrumentos Vuelco de almacenamiento dinámico y/o Análisis de memoria, necesita habilitar el recopilador de datos para la recopilación de instantáneas de almacenamiento dinámico y/o la recopilación de asignación de memoria, lo que se puede hacer en los archivos `.properties` del recopilador de datos. Consulte "Personalización del recopilador de datos con archivos de propiedades" en la página 921.
- Si el archivo de claves o el Servidor de Cloud APM cambian, vuelva a conectar el recopilador de datos al Servidor de Cloud APM. Para obtener instrucciones, consulte "Reconexión del recopilador de datos al Servidor de Cloud APM" en la página 193.

Variables de entorno para personalizar el recopilador de datos de Liberty
Para personalizar el recopilador de datos de Liberty para las aplicaciones IBM Cloud, utilice la interfaz de usuario de IBM Cloud para añadir las variables de entorno soportadas por el recopilador de datos.

Consejo: Para añadir variables de entorno en la IU de IBM Cloud, primero inicie la sesión en la IU de IBM Cloud, pulse la aplicación y, a continuación, pulse **Tiempo de ejecución** > **Variable de entorno**. En la sección **definidas por el usuario**, añada las variables de entorno.

- Utilice las variables listadas en Tabla 228 en la página 919 para configurar la conexión entre el recopilador de datos de Liberty y el Servidor de Cloud APM.
- Utilice la variable listada en Tabla 229 en la página 920 para habilitar o inhabilitar el rastro de métodos para sus aplicaciones IBM Cloud.
- Una vez habilitado el rastreo de métodos, utilice las variables listadas en Tabla 230 en la página 920 para especificar los umbrales para diferentes tipos de solicitudes de modo que se puedan recopilar diferentes niveles de datos de supervisión.

Recuerde: Después de añadir o modificar la variable de entorno, reinicie la aplicación para que los cambios surtan efecto.

Tabla 228. Variables de entorno para conexiones de servidor

Nombre de variable	Valores posibles	Descripción
APM_BM_GATEWAY_URL	• `https://` *`ip_o_nombre_host_servidor`* `:443` • `http://` *`ip_o_nombre_host_servidor`* `:80`	El URL de la pasarela del Servidor de Cloud APM de destino.
APM_KEYFILE_PSWD	Contraseña cifrada del archivo de claves	La contraseña del archivo de claves cifrada que se empareja con el archivo de claves. Si es usuario de Linux, puede utilizar el mandato `echo -n` *`<contraseña de archivo de claves>`* `| base64` para cifrar la contraseña. **Recuerde:** establezca esta variable sólo cuando haya configurado la variable *APM_BM_GATEWAY_URL* para utilizar HTTPS.
APM_KEYFILE_URL	`http://` *`servidor_http_alojado:puerto`*`/keyfile.jks`	El URL utilizado para descargar el archivo de claves. **Recuerde:** establezca esta variable sólo cuando haya configurado la variable *APM_BM_GATEWAY_URL* para utilizar HTTPS.

Tabla 229. Variable de entorno para rastreo de métodos		
Nombre de variable	**Valores posibles**	**Descripción**
METHOD_TRACE_ENABLE	• `verdadero` • `falso`	Utilice esta variable para habilitar o inhabilitar el rastreo de métodos. El valor `true` habilita el rastreo de métodos. El valor predeterminado es `false`.

Una vez habilitado el rastreo de método, puede configurar umbrales para diferentes tipos de solicitudes a fin de personalizar el rastreo de método. Pueden configurarse los siguientes umbrales, que desencadenan la recopilación de diferentes niveles de datos supervisión, para cada tipo de solicitud:

Umbrales primarios
Si configura el umbral primario para un tipo de solicitud, se captura la información de temporización de este tipo de solicitudes, como por ejemplo tiempo de CPU y el tiempo de respuesta. Como resultado, cuando una solicitud tarda más en completarse que el tiempo especificado para el umbral primario, se captura la temporización de la solicitud.

Umbrales secundarios
Si configura el umbral secundario para un tipo de solicitud, se capturan datos de contexto profundo, como por ejemplo rastreos de pila y SQL para solicitudes de base de datos. Los datos de contexto que se capturan difieren en función del tipo de solicitud. Cuando una solicitud tarda más tiempo en finalizar que el tiempo que se ha especificado para el umbral secundario, se capturan sus datos de contexto.

La variable de entorno para diferentes umbrales de solicitud se denomina según el formato *<tipo_solicitud>_<nivel de umbral>*. Por ejemplo, para configurar un umbral primario para la solicitud JMS, añada la variable JMS_PRIMARY y establezca el valor correspondiente.

Tabla 230 en la página 920 lista las variables de entorno correspondientes que puede añadir para diferentes tipos de solicitud. Los valores se expresan en milisegundos.

Tabla 230. Variables de entorno para diferentes umbrales de solicitud	
Nombre de variable	**Valor predeterminado (en milisegundos)**
SERVLET_PRIMARY	20
SERVLET_SECONDARY	50
JDBC_PRIMARY	20
JDBC_SECONDARY	50
JNDI_PRIMARY	20
JNDI_SECONDARY	50
EJB_PRIMARY	20
EJB_SECONDARY	50
WEBSERVICES_PRIMARY	20
WEBSERVICES_SECONDARY	50
APP_METHODS_PRIMARY (métodos de aplicación – no J2EE)	50
APP_METHODS _SECONDARY	1000
JCA_PRIMARY	50
JCA_SECONDARY	80

Tabla 230. Variables de entorno para diferentes umbrales de solicitud (continuación)	
Nombre de variable	**Valor predeterminado (en milisegundos)**
JMS_PRIMARY	40
JMS_SECONDARY	70

Personalización del recopilador de datos con archivos de propiedades

De forma predeterminada, el rastreo de transacciones y el rastreo de métodos están habilitados para el recopilador de datos. La recopilación de instantáneas de almacenamiento dinámico y la recopilación de asignación de memoria están inhabilitadas. Puede personalizar la recopilación de datos o los intervalos a los que se recopilan los datos de diagnóstico editando los archivos `.properties` del recopilador de datos.

Acerca de esta tarea

Los archivos de propiedades del recopilador de datos están en el directorio *inicio_dc*, por ejemplo `/opt/liberty855/wlp/usr/servers/defaultServer/.gdc/7.3.0.14.08`. Utilice diferentes propiedades para personalizar el recopilador de datos a los efectos siguientes:

- Habilitar o inhabilitar el rastreo de transacciones.
- Habilitar o inhabilitar la recopilación de instantáneas de almacenamiento dinámico.
- Especificar el intervalo de toma de instantáneas del vuelco de almacenamiento dinámico por parte del recopilador de datos.
- Habilitar o inhabilitar la supervisión de asignación de memoria.
- Especificar el intervalo de recopilación de información de asignación de memoria por parte del recopilador de datos.
- Habilitar o inhabilitar el rastreo de métodos.

Recuerde: Después de modificar los archivos `.properties`, utilice el mandato **`cf push`** para enviar las actualizaciones al entorno IBM Cloud.

Procedimiento

- Para habilitar o inhabilitar el rastreo de transacciones, establezca la propiedad **`com.ibm.tivoli.itcam.dc.bluemix.transaction.enabled`** en `true` o `false` en el archivo siguiente:

  inicio_dc`/ldc/etc/ldc.properties`

  Si el rastreo de transacciones está habilitado, puede supervisar la pila de aplicaciones IBM Java en las topologías.
- Para habilitar o inhabilitar la recopilación de instantáneas de almacenamiento dinámico, establezca las propiedades **`com.ibm.tivoli.itcam.hc.send.heap.enable`** y **`com.ibm.tivoli.itcam.hc.snapshot.automatic.enable`** en `true` o `false` en el archivo siguiente.

  inicio_dc`/healthcenter/etc/hc.properties`

  Si la recopilación de instantáneas de almacenamiento dinámico está habilitada, el recopilador de datos puede tomar una instantánea de almacenamiento dinámico a intervalos especificados. La información de vuelco de almacenamiento dinámico se puede visualizar en el panel de instrumentos Vuelco de almacenamiento dinámico.
- Para cambiar el intervalo de toma de instantáneas de almacenamiento dinámico por parte del recopilador de datos, establezca la propiedad **`com.ibm.tivoli.itcam.hc.snapshot.automatic.interval`** en un entero positivo en el mismo archivo. La unidad del intervalo son los minutos y el valor predeterminado es `360`.

  inicio_dc`/healthcenter/etc/hc.properties`

- Para habilitar o inhabilitar la recopilación de asignación de memoria, establezca la propiedad **com.ibm.tivoli.itcam.hc.events.collection.automatic.enable** en `true` o `false` en el archivo siguiente.

  inicio_dc`/healthcenter/etc/hc.properties`

  Recuerde: Para habilitar la recopilación de asignación de memoria, también debe asegurarse de que se añaden las dos líneas siguientes al archivo `jvm.options` del servidor Liberty.

  ```
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  ```

  Una vez habilitada la recopilación de asignación de memoria, hay datos disponibles en el panel de instrumentos de Análisis de memoria.
- Para especificar el intervalo de recopilación de información de asignación de memoria, establezca la propiedad **com.ibm.tivoli.itcam.hc.events.collection.automatic.interval** en un entero positivo en el mismo archivo. La unidad del intervalo son los minutos y el valor predeterminado es 15.

  inicio_dc`/healthcenter/etc/hc.properties`
- Para habilitar o inhabilitar el rastreo de métodos, establezca la propiedad **dfe.enable.methoddata** en `true` o `false` en el archivo siguiente:

  inicio_dc`/gdc/etc/gdc_dfe.properties`

Qué hacer a continuación

- Una vez habilitado el rastreo de métodos, puede establecer umbrales para diferentes tipos de solicitudes mediante las variables de entorno de modo que se puedan recopilar diferentes niveles de datos de supervisión para diferentes solicitudes. Para variables de entorno aplicables, consulte Tabla 230 en la página 920.
- Si ha inhabilitado la recopilación de asignación de memoria, acuérdese de eliminar las líneas siguientes del archivo `jvm.options` del servidor Liberty:

  ```
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  ```

Desconfiguración del recopilador de datos para aplicaciones IBM Cloud

Si no necesita supervisar perfiles de Liberty en el entorno IBM Cloud o si desea actualizar el recopilador de datos a una versión nueva, debe desconfigurar el recopilador de datos que ha desplegado anteriormente.

Acerca de esta tarea

Para desconfigurar el recopilador de datos para el perfil de Liberty en el entorno IBM Cloud, retrotraiga los cambios realizados en los archivos `jvm.options`, `server.env` y `server.xml` y actualice el perfil de Liberty en IBM Cloud con el mandato **`cf push`**.

Procedimiento

1. En el directorio local del perfil de Liberty, modifique el archivo `jvm.options` para eliminar los parámetros siguientes. Puede suprimir el archivo si está vacío después del cambio.

   ```
   -agentlib:am_ibm_16=defaultServer
   -Xbootclasspath/p:../../../../.gdc/7.3.0.14.08/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=../../../../.gdc/7.3.0.14.08/itcamdc/etc/datacollector
   .policy
   -Dliberty.home=/home/vcap/app/.liberty
   -Xhealthcenter:level=inprocess
   -Xgc:allocationSamplingGranularity=10000
   -verbosegc
   -Xverbosegclog:/home/vcap/app/wlp/usr/servers/defaultServer/logs/gc.log,1,10000
   ```

2. En el archivo `server.env`, elimine el valor siguiente de la variable de entorno **LD_LIBRARY_PATH**. Puede suprimir el archivo si está vacío después del cambio.

```
LD_LIBRARY_PATH=:/lib:../../../../.gdc/7.3.0.14.08/toolkit/lib/lx8266
:../../../../.gdc/7.3.0.14.08/toolkit/lib/lx8266/ttapi
```

3. Modifique el archivo `server.xml` para eliminar la característica monitor-1.0 eliminando la línea siguiente de la sección `<featureManager>`

```
<feature>monitor-1.0</feature>
```

4. Suprima el directorio `.gdc` dentro del directorio de inicio de Liberty.
5. Abra un indicador de mandatos, sitúese en el directorio que contiene el archivo `manifest.yml` del servidor Liberty.
6. Inicie la sesión en IBM Cloud y actualice el perfil de Liberty con el mandato **`cf push`**.

Qué hacer a continuación
Tras desconfigurar el recopilador de datos, la Consola de Cloud APM continúa mostrando el recopilador de datos en cualquier aplicación a la que haya añadido el recopilador de datos. La Consola de Cloud APM mostrará que no hay datos disponibles para la aplicación y no indicará que el recopilador de datos está fuera de línea. Para obtener información sobre cómo eliminar el recopilador de datos de aplicaciones y de grupos de recursos, consulte "Eliminación de recopiladores de datos de Consola de Cloud APM" en la página 196.

Configuración avanzada del recopilador de datos

Puede modificar los archivos de configuración del recopilador de datos para cambiar los valores adicionales de supervisión.

Archivos de propiedades para el recopilador de datos de Liberty

Se proporcionan varios archivos de configuración para controlar la configuración y el comportamiento del recopilador de datos.

Después de extraer el paquete de recopilador de datos en un directorio local, los archivos del recopilador de datos están ubicados en el directorio *dir_local*`/liberty_dc/.gdc/7.3.0.14.08`. Por ejemplo `/opt/ibm/apm/.gdc/7.3.0.14.08`. Esta carpeta se convierte en el directorio de inicio del recopilador de datos que a efectos de simplificación se indica como *inicio_dc* en las declaraciones siguientes.

Archivos de propiedades del recopilador de datos

Cada instancia de servidor de aplicaciones supervisada por el recopilador de datos tiene sus propias propiedades. El recopilador de datos crea automáticamente el archivo de propiedades. El nombre del archivo es *dir_inicio_dc*`/runtime/`*versión_servidor_aplic.nombre_nodo.nombre_perfil.nombre_servidor*`/datacollector.properties`.

Para facilitar futuras actualizaciones, no cambie este archivo.

En su lugar, añada los valores que desea modificar al archivo de propiedades personalizado del recopilador de datos. Este archivo se denomina *dir_inicio_dc*`/runtime/`*versión_servidor_apl.nombre_nodo.nombre_perfil.nombre_servidor*`/custom/datacollector_custom.properties`. Los valores del archivo de propiedades personalizado del recopilador de datos alteran temporalmente los valores que hay en el archivo de propiedades del recopilador de datos.

Importante: Si el archivo *dir_inicio_dc*`/runtime/`*versión_servidor_aplic.nombre_nodo.nombre_perfil.nombre_servidor*`/custom/datacollector_custom.properties` no existe, créelo cuando desee realizar cambios. Es posible que también tenga que crear el directorio `custom`.

Archivo de propiedades del kit de herramientas

El archivo de propiedades del kit de herramientas lo crea automáticamente el recopilador de datos durante el inicio, utilizando varios archivos de entrada. Es exclusivo para cada instancia de servidor de aplicaciones supervisada por el recopilador de datos. El nombre del archivo es *dir_inicio_dc*/runtime/*versión_servidor_aplic.nombre_nodo.nombre_perfil.nombre_servidor*/toolkit.properties.

Dado que este archivo se vuelve a crear en cada inicio del recopilador de datos, **no realice ningún cambio** en este archivo; si lo hace, los cambios se sobrescribirán.

En su lugar, añada los valores que desee modificar al archivo de propiedades personalizado del kit de herramientas. Este archivo se denomina *dir_inicio_dc*/runtime/*versión_servidor_apl.nombre_nodo.nombre_perfil.nombre_servidor*/custom/toolkit_custom.properties. Los valores del archivo de propiedades personalizado del kit de herramientas sustituyen a los valores del archivo de propiedades del kit de herramientas.

También puede establecer propiedades del kit de herramientas para todas las instancias de servidor de aplicaciones supervisadas por esta instalación del recopilador de datos. Para ello, añada los valores al archivo de propiedades personalizado global del kit de herramientas: *dir_inicio_dc*/runtime/custom/toolkit_global_custom.properties. Sin embargo, si se establece una propiedad en el archivo toolkit_custom.properties específico de la instancia, sustituye al valor en el archivo global para esta instancia.

Importante: Si el archivo *dir_inicio_dc*/runtime/*versión_servidor_aplic.nombre_nodo.nombre_perfil.nombre_servidor*/custom/toolkit_custom.properties o *dir_inicio_dc*/runtime/custom/toolkit_custom.properties no existe, créelo cuando desee realizar cambios. Es posible que también tenga que crear el directorio custom.

Otros archivos de propiedades

Además del archivo de propiedades del recopilador de datos y el archivo de propiedades del kit de herramientas, hay otros archivos de propiedades que son exclusivos para cada instancia de servidor de aplicaciones supervisada por el recopilador de datos:

***dir_inicio_dc*/runtime/*appserver_versión.nombre_nodo.nombre_perfil.nombre_servidor*/custom/gdc/gdc_custom.properties**
: Define los detalles para recopilar los datos de seguimiento de método y de diagnóstico. Para obtener más información acerca de este archivo, consulte "Configuración de la recopilación de información de diagnóstico detallada" en la página 927.

***dir_inicio_dc*/runtime/*appserver_versión.nombre_nodo.nombre_servidor*/hc.properties**
: Define los detalles de la recopilación de instantáneas de almacenamiento dinámico y la recopilación de asignación de memoria. Para obtener más información acerca de este archivo, consulte "Configuración de la recopilación de información de diagnóstico detallada" en la página 927.

***dir_inicio_dc*/runtime/*appserver_versión.nombre_nodo.nombre_perfil.nombre_servidor*/cynlogging.properties**
: Define los nombres de archivo de registro y los detalles de registro de la parte Java del recopilador de datos.

***dir_inicio_dc*/runtime/*appserver_versión.nombre_nodo.nombre_perfil.nombre_servidor*/cyncclog.properties**
: Define los nombres de archivo de registro y los detalles de registro de la parte C++ del recopilador de datos.

Archivos de rastreo del recopilador de datos

Los archivos de rastreo del recopilador de datos se almacenan de forma predeterminada en las siguientes ubicaciones:

- Windows *dir_inicio_dc*\logs\CYN\logs.
- Linux AIX *dir_inicio_dc*/logs/CYN/logs.

Habilitación o inhabilitación del rastreo de transacciones y la recopilación de datos de diagnóstico
De forma predeterminada, el rastreo de transacciones y el rastreo de métodos están habilitados para el recopilador de datos. La recopilación de instantáneas de almacenamiento dinámico y la recopilación de asignación de memoria están inhabilitadas. Puede personalizar la recopilación de datos o los intervalos a los que se recopilan los datos de diagnóstico editando los archivos `.properties` del recopilador de datos.

Acerca de esta tarea

Los archivos de propiedades del recopilador de datos están en el directorio *inicio_dc*, por ejemplo `/opt/ibm/apm/.gdc/7.3.0.14.08`. Utilice diferentes propiedades para personalizar el recopilador de datos a los efectos siguientes:

- Habilitar o inhabilitar el rastreo de transacciones.
- Habilitar o inhabilitar la recopilación de instantáneas de almacenamiento dinámico.
- Especificar el intervalo de toma de instantáneas del vuelco de almacenamiento dinámico por parte del recopilador de datos.
- Habilitar o inhabilitar la supervisión de asignación de memoria.
- Especificar el intervalo de recopilación de información de asignación de memoria por parte del recopilador de datos.
- Habilitar o inhabilitar el rastreo de métodos.

Recuerde: En función de si ha reiniciado o no el servidor Liberty después de la configuración del recopilador de datos, hay diferentes archivos `.properties` aplicables. Si ha reiniciado el servidor Liberty después de la configuración del recopilador de datos, se crea un directorio `runtime` en el directorio *inicio_dc*. Después de eso, solo puede utilizar los archivos `.properties` que hay dentro del directorio *inicio_dc*`/runtime/`*appserver_versión.nombre_nodo.nombre_perfil.nombre_servidor* para personalizar el recopilador de datos para cada servidor de aplicaciones.

Procedimiento

- Para habilitar o inhabilitar el rastreo de transacciones, establezca la propiedad **com.ibm.tivoli.itcam.dc.bluemix.transaction.enabled** en `true` o `false` en el archivo siguiente:

  inicio_dc`/runtime/`*appserver_versión.nombre_nodo.nombre_servidor*`/ldc.properties` (si el directorio `runtime` no existe,utilice *inicio_dc*`/ldc/etc/ldc.properties`)

  Una vez habilitado el rastreo de transacciones, puede supervisar la pila de aplicaciones IBM Java en las topologías.
- Para habilitar o inhabilitar la recopilación de instantáneas de almacenamiento dinámico, establezca las propiedades **com.ibm.tivoli.itcam.hc.send.heap.enable** y **com.ibm.tivoli.itcam.hc.snapshot.automatic.enable** en `true` o `false` en el archivo siguiente.

  inicio_dc`/runtime/`*appserver_versión.nombre_nodo.nombre_servidor*`/hc.properties` (si el directorio `runtime` no existe,utilice *inicio_dc*`/healthcenter/etc/hc.properties`)

Una vez habilitada la recopilación de instantáneas de almacenamiento dinámico, el recopilador de datos puede tomar una instantánea de almacenamiento dinámico a intervalos especificados. La información de vuelco de almacenamiento dinámico se puede visualizar en el panel de instrumentos Vuelco de almacenamiento dinámico.

- Para cambiar el intervalo de toma de instantáneas de almacenamiento dinámico por parte del recopilador de datos, establezca la propiedad **com.ibm.tivoli.itcam.hc.snapshot.automatic.interval** en un entero positivo en el mismo archivo. La unidad del intervalo son los minutos y el valor predeterminado es 360.

  inicio_dc/runtime/*appserver_versión.nombre_nodo.nombre_servidor*/hc.properties (si el directorio runtime no existe,utilice *inicio_dc*/healthcenter/etc/hc.properties)

- Para habilitar o inhabilitar la recopilación de asignación de memoria, establezca la propiedad **com.ibm.tivoli.itcam.hc.events.collection.automatic.enable** en true o false en el archivo siguiente.

  inicio_dc/runtime/*appserver_versión.nombre_nodo.nombre_servidor*/hc.properties (si el directorio runtime no existe,utilice *inicio_dc*/healthcenter/etc/hc.properties)

  Recuerde: Para habilitar la recopilación de asignación de memoria, también debe asegurarse de que se añaden las dos líneas siguientes al archivo jvm.options del servidor Liberty.

  ```
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  ```

  Una vez habilitada la recopilación de asignación de memoria, hay datos disponibles en el panel de instrumentos de Análisis de memoria.

- Para especificar el intervalo de recopilación de información de asignación de memoria, establezca la propiedad **com.ibm.tivoli.itcam.hc.events.collection.automatic.interval** en un entero positivo en el mismo archivo. La unidad del intervalo son los minutos y el valor predeterminado es 15.

  inicio_dc/runtime/*appserver_versión.nombre_nodo.nombre_servidor*/hc.properties (si el directorio runtime no existe,utilice *inicio_dc*/healthcenter/etc/hc.properties)

- Para habilitar o inhabilitar el rastreo de métodos, establezca la propiedad **dfe.enable.methoddata** en true o false en el archivo siguiente:

  inicio_dc/runtime/*appserver_versión.nombre_nodo.nombre_perfil.nombre_servidor*/custom/gdc/gdc_custom.properties (si el directorio runtime no existe, utilice *inicio_dc*/gdc/etc/gdc_dfe.properties)

Resultados

Después de modificar los archivos .properties, reinicie el servidor Liberty para que los cambios surtan efecto.

Para obtener más información sobre los archivos del recopilador de datos .properties para cada servidor de aplicaciones, consulte "Archivos de propiedades para el recopilador de datos de Liberty" en la página 923.

Qué hacer a continuación

- Una vez habilitado el rastreo de métodos, puede establecer umbrales para diferentes tipos de solicitudes de modo que se puedan recopilar diferentes niveles de datos de supervisión para diferentes solicitudes. Para obtener instrucciones, consulte "Personalización de los umbrales de solicitud" en la página 929.

- Si ha inhabilitado la recopilación de asignación de memoria, acuérdese de eliminar las líneas siguientes del archivo `jvm.options` del servidor Liberty:

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
```

Configuración de la recopilación de información de diagnóstico detallada
Si tiene IBM Cloud Application Performance Management, Advanced, puede utilizar el recopilador de datos para recopilar la información de diagnóstico detallada en la instancia del servidor de la aplicación supervisada. Para configurar el comportamiento de la colección de datos de diagnóstico, incluyendo la cantidad de información de diagnóstico que almacena el recopilador de datos, personalice el archivo de configuración `gdc_custom.properties`.

Acerca de esta tarea

Puede encontrar el archivo `gdc_custom.properties` en el directorio *dir_inicio_dc*`/runtime/`*versión_servidor_aplic.nombre_nodo.nombre_perfil.nombre_servidor*`/custom/gdc`.

Los ejemplos siguientes describen cómo utilizar las propiedades en el archivo de configuración `gdc_custom.properties` para hacer lo siguiente:

- Definición de límites para el tamaño y el número de archivos de información detallada
- Establecimiento de la recopilación completa o parcial de datos de diagnóstico de método y solicitud

También puede establecer otras propiedades en el archivo `gdc_custom.properties` para personalizar la recopilación de datos de diagnóstico. Consulte los comentarios en el archivo que describen las propiedades.

Recuerde: Después de completar la edición del archivo `gdc_custom.properties`, debe reiniciar la instancia del servidor de aplicaciones supervisada para que los cambios entren en vigor.

Definición de límites para el tamaño y el número de archivos de información detallada

Acerca de esta tarea

El recopilador de datos almacena información de diagnóstico en diversos archivos. De forma predeterminada almacena 100 archivos; si hay 10 archivos almacenados y se crea uno nuevo, se suprimirá el archivo con más antigüedad. El recopilador de datos crea un archivo nuevo cada 15 minutos, o cuando el tamaño del archivo actual sobrepasa los 200 megabytes. Cuando el tamaño total del directorio que contiene los archivos sobrepasa los 2 gigabytes, el recopilador de datos suprime el archivo con más antigüedad.

Procedimiento

Puede modificar los siguientes valores del archivo *dir_inicio_dc*`/runtime/`*versión_servidor_aplic.nombre_nodo.nombre_perfil.nombre_servidor*`/custom/gdc/gdc_custom.properties`:

- Para establecer el número máximo de archivos con información de diagnóstico, establezca la propiedad `com.ibm.itcam.gdc.dfe.filelimit`.
  Por ejemplo:

```
com.ibm.itcam.gdc.dfe.filelimit=100
```

- Para establecer el tiempo, en minutos, transcurrido el cual el recopilador de datos crea un nuevo archivo de datos de diagnóstico, establezca la propiedad `com.ibm.itcam.gdc.dfe.frequency`.
  Por ejemplo:

```
com.ibm.itcam.gdc.dfe.frequency=15
```

- Para establecer el tamaño máximo del archivo de datos de diagnóstico, en megabytes, establezca la propiedad `dfe.file.maxlimit`.

Por ejemplo:

```
dfe.file.maxlimit=200
```

Si el archivo de datos de diagnóstico actual alcanza este tamaño, el recopilador de datos crea un nuevo archivo de datos de diagnóstico.

- Para establecer el tamaño máximo total de todos los archivos de datos, en bytes, establezca la propiedad `trace.dir.size.limit`.
  Por ejemplo:

  ```
  trace.dir.size.limit=2147483648
  ```

  Si la suma de los tamaños de todos los archivos de datos de diagnóstico sobrepasa este valor, el recopilador de datos suprime el archivo de datos con más antigüedad. El tamaño máximo total es de 25 megabytes.

Establecimiento de la recopilación completa o parcial de datos de diagnóstico de método y solicitud

Acerca de esta tarea

El recopilador de datos tiene los siguientes valores predeterminados:

- El recopilador de datos recopila datos de diagnóstico solo para las solicitudes seleccionadas. La selección (muestreo) de las solicitudes tiene como objetivo incluir todos los errores y algunas solicitudes correctas.
- La recopilación de datos de método está inhabilitada cuando se inicia el servidor.
- Cuando la recopilación de datos de método está habilitada, el recopilador de datos recopila datos de método sólo para algunas solicitudes (de aquellas para las que se recopilan datos de diagnóstico). Este selección adicional (muestreo) tiene como objetivo incluir todos los errores y algunas solicitudes correctas.

Importante: La modificación de estos valores afecta al rendimiento del servidor de aplicaciones. En los servidores de producción, la degradación del rendimiento puede ser crítica.

Procedimiento

Puede modificar estos valores utilizando las propiedades del archivo *dir_inicio_dc*`/runtime/`*versión_servidor_aplic.nombre_nodo.nombre_perfil.nombre_servidor*`/custom/gdc/gdc_custom.properties`.

- Para habilitar la recopilación de datos de método, establezca la propiedad como se indica a continuación:

  ```
  dfe.enable.methoddata=true
  ```

  Consejo: También puede utilizar la página **Configuración de agente** para habilitar o inhabilitar dinámicamente la recopilación de datos de rastreo de método.
- Para recopilar datos de diagnóstico para cada solicitud, inhabilite el muestreo estableciendo la propiedad como se indica a continuación:

  ```
  dc.sampling.enable=false
  ```

- Para habilitar la recopilación de datos de método para cada solicitud para la que se recopilan datos de diagnóstico, establezca la propiedad de esta manera:

  ```
  dc.sampling.enable=false
  dc.sampling.methsampler.enabled=false
  ```

  Recuerde: La propiedad `dc.sampling.methsampler.enabled` solo tiene efecto cuando la recopilación de datos de método está habilitada en la página Configuración del agente o por la propiedad `dfe.enable.methoddata`.

Personalización de los umbrales de solicitud
Algunas de las solicitudes quizá no tengan suficiente información si los umbrales predeterminados son altos. Puede personalizar los umbrales de solicitud de forma que el recopilador de datos pueda capturar más datos de contexto de solicitud o solicitudes.

Acerca de esta tarea

Cada tipo de solicitud tiene dos tipos de umbral, denominados **perfThreshold** y **secondaryPerfThreshold**. El recopilador de datos captura una solicitud solo cuando toma más tiempo del especificado para el umbral **perfThreshold**. Los datos de contexto, como seguimiento de la pila y sentencia SQL, solo se capturan cuando la solicitud toma más tiempo del especificado para el umbral **secondaryPerfThreshold**. Puede ajustar estos valores de umbral para satisfacer sus necesidades.

Procedimiento

1. Vaya al directorio *inicio_dc*\gdc\etc, donde *inicio_dc* es el directorio de inicio del recopilador de datos.
2. En un editor de texto, abra el archivo XML para el tipo de solicitud que desea personalizar. Puede ver qué archivo es para el tipo de solicitud en el nombre del archivo XML.
   Por ejemplo, el archivo `ejb.xml` es para solicitudes EJB, el archivo `custom.xml` es para solicitudes personalizadas y el archivo `appMethods.xml` es para clases y métodos cuando el rastreo de método está habilitado.
3. Establezca los códigos <collectContextData>, <collectStackTrace> y <createDataRow> en ifThresholdExceeded.

```
<collectContextData>ifThresholdExceeded</collectContextData>
<collectStackTrace>ifThresholdExceeded</collectStackTrace>
<createDataRow>ifThresholdExceeded</createDataRow>
```

4. Establezca los códigos <perfThreshold> y <secondaryPerfThreshold> en los valores de umbral que desee. La unidad del umbral es milisegundos.
   Por ejemplo, el archivo `ejb.xml` tiene los valores siguientes para solicitudes EJB. Como resultado, el recopilador de datos solo captura las solicitudes EJB que toman más de 1 segundo (1000 milisegundos). Además, los datos de contexto relacionados con la solicitud EJB, como el seguimiento de la pila e inicio EJB, solo se capturan cuando la solicitud EJB toma más de 1,5 segundos (1500 milisegundos).

```
<requestProbePoint id="EJB">
<interface>com.ibm.tivoli.itcam.toolkit.ai.boot.aspectmanager.ITurboEJBEventListener</
interface>
<family>EJB</family>
<collectContextData>ifThresholdExceeded</collectContextData>
<collectStackTrace>ifThresholdExceeded</collectStackTrace>
<perfThreshold>1000</perfThreshold>
<secondaryPerfThreshold>1500</secondaryPerfThreshold>
<dataToCollect>instanceAndSummary</dataToCollect>
<createDataRow>ifThresholdExceeded</createDataRow>
<requestType>EJB Method</requestType>
</requestProbePoint>
```

5. Guarde los cambios y reinicie el servidor de aplicaciones.

Inhabilitación de diversos tipos de Instrumentación de códigos de bytes para las API de Java EE
En la instrumentación de código de bytes (BCI), el recopilador de datos intercepta las llamadas de entrada y salida del método para diversos tipos de API de Java Platform Enterprise Edition (Java EE) para crear un flujo de ejecución para cada solicitud de aplicación. Algunos recursos se utilizan para la supervisión. Puede ajustar el recopilador de datos de forma que algunas de las API no se supervisen, reduciendo el uso de los recursos.

Para inhabilitar la supervisión de BCI para las API de Java EE, añada las propiedades siguientes al archivo de propiedades personalizadas del kit de herramientas. Para obtener más información acerca de este archivo, consulte “Archivo de propiedades del kit de herramientas” en la página 924.

Tabla 231. Adición de líneas al archivo de propiedades personalizadas del kit de herramientas

Tipo de API de Java EE	**Línea que debe añadirse al archivo `toolkit_custom.properties`**
Enterprise JavaBeans (EJB)	`com.ibm.tivoli.itcam.toolkit.ai.enableejb=false`
Java Connector Architecture (JCA)	`com.ibm.tivoli.itcam.toolkit.ai.enablejca=false`
Java Database Connectivity (JDBC)	`com.ibm.tivoli.itcam.toolkit.ai.enablejdbc=false`
Java Naming and Directory Interface (JNDI)	`com.ibm.tivoli.itcam.toolkit.ai.enablejndi=false`
Java Message Service (JMS)	`com.ibm.tivoli.itcam.toolkit.ai.enablejms=false`
Contenedores web para Servlets/JavaServer Pages (JSP)	`com.ibm.tivoli.itcam.dc.was.webcontainer=false`
Seguimiento de recuento de sesiones HTTP	`com.ibm.tivoli.itcam.toolkit.ai.enablesessioncount=false`
CICS Transaction Gateway (CTG)	`com.ibm.tivoli.itcam.dc.ctg.enablectg=false`
IMS	`com.ibm.tivoli.itcam.dc.mqi.enableims=false`
Java Data Objects (JDO)	`com.ibm.tivoli.itcam.dc.mqi.enablejdo=false`
Interfaz de cola de mensajes (MQI)	`com.ibm.tivoli.itcam.dc.mqi.enablemqi=false`
Servicio web de Axis	`com.ibm.tivoli.itcam.toolkit.ai.axis.enablewebservice=false`
Invocación a método remoto (RMI)	`am.ejb.rmilistener.enable=false`
Contenedor EJB de WebSphere Application Server	`com.ibm.tivoli.itcam.dc.was.enableEJBContainer=false`

Inhabilitación del rastreo de transacciones para un cierto tipo de transacciones

Cuando el rastreo de transacciones está inhabilitado para el recopilador de datos, de forma predeterminada se supervisan todos los tipos de transacciones. Puede utilizar el archivo de propiedades del kit de herramientas para inhabilitar el rastreo de transacciones para tipos de transacciones específicos.

Acerca de esta tarea

Edite el archivo `toolkit_custom.properties` para personalizar el rastreo de transacciones para cada servidor de aplicaciones o edite el archivo `toolkit_global_custom.properties` para todas las instancias del servidor de aplicaciones.

El archivo `toolkit_custom.properties` se utiliza en el procedimiento siguiente para un solo servidor de aplicaciones. Las propiedades también están soportadas en el archivo `toolkit_global_custom.properties`. Para obtener más información acerca de los archivos de

propiedades del kit de herramientas, consulte Archivos de propiedades para el recopilador de datos de Liberty.

Procedimiento

1. Abra el archivo `toolkit_custom.properties` del servidor de aplicaciones con un editor de texto. Este archivo se puede encontrar en el directorio siguiente:

   dir_inicio_dc/runtime/*versión_servidoraplicaciones.nombre_nodo.nombre_perfil.nombre_servidor*/custom
2. Según sus necesidades, especifique una o varias de las propiedades siguientes y establezca el valor de la propiedad en `false` para inhabilitar el rastreo de transacciones para un cierto tipo de transacciones.

   Para solicitudes de CICS
   `com.ibm.tivoli.itcam.dc.ttapi.cics.enabled=false`

   Para solicitudes personalizadas
   `com.ibm.tivoli.itcam.dc.ttapi.ims.enabled=false`

   Para solicitudes de EJB
   `com.ibm.tivoli.itcam.dc.ttapi.ejb.enabled=false`

   Para llamadas de cliente HTTP
   `com.ibm.tivoli.itcam.dc.ttapi.httpclient.enabled=false`

   Excepción: Para inhabilitar el rastreo de transacciones para llamadas de Apache HTTP Client, especifique `com.ibm.tivoli.itcam.toolkit.dc.enable.apache.httpclient=false`.

   Para solicitudes de IMS
   `com.ibm.tivoli.itcam.dc.ttapi.ims.enabled=false`

   Para solicitudes de JDBC
   `com.ibm.tivoli.itcam.dc.ttapi.jdbc.enabled=false`

   Para solicitudes de JMS
   `com.ibm.tivoli.itcam.dc.ttapi.jms.enabled=false`

   Para solicitudes de JNDI
   `com.ibm.tivoli.itcam.dc.ttapi.jndi.enabled=false`

   Para solicitudes de MQI
   `com.ibm.tivoli.itcam.dc.ttapi.mqi.enabled=false`

   Para solicitudes de Portal
   `com.ibm.tivoli.itcam.dc.ttapi.portal=false`

   Para solicitudes de RMI-IIOP
   `com.ibm.tivoli.itcam.dc.ttapi.rmiiiop.enabled=false`

   Para solicitudes de Servlet
   `com.ibm.tivoli.itcam.dc.ttapi.arm.servlet.enabled=false`

   Para solicitudes de servicio web
   `com.ibm.tivoli.itcam.dc.ttapi.webservice.enabled=false`

   Consejo: Para obtener más información sobre estas propiedades, consulte el archivo *dir_inicio_dc*/ttdc/etc/ttdc.properties.
3. Guarde y cierre el archivo `toolkit_custom.properties`.
4. Reinicie el servidor de aplicaciones para que los cambios entren en vigor.

Exclusión de clases de la supervisión
Puede personalizar la recopilación de datos excluyendo ciertas clases de la supervisión. Utilice el archivo de propiedades del kit de herramientas para esta personalización.

Acerca de esta tarea

Edite el archivo `toolkit_custom.properties` para personalizar el rastreo de transacciones para cada servidor de aplicaciones o edite el archivo `toolkit_global_custom.properties` para todas las instancias del servidor de aplicaciones.

El archivo `toolkit_custom.properties` se utiliza en el procedimiento siguiente para un solo servidor de aplicaciones. Las propiedades también están soportadas en el archivo `toolkit_global_custom.properties`. Para obtener más información acerca de los archivos de propiedades del kit de herramientas, consulte Archivos de propiedades para el recopilador de datos de Liberty.

Procedimiento

1. Abra el archivo `toolkit_custom.properties` del servidor de aplicaciones con un editor de texto. Este archivo se puede encontrar en el directorio siguiente:

   dir_inicio_dc/runtime/*versión_servidoraplicaciones.nombre_nodo.nombre_perfil.nombre_servidor*/custom
2. Edite el archivo para añadir la propiedad siguiente y guarde los cambios.

   ```
   am.camtoolkit.gpe.customxml.exclude=excludes.xml
   ```
3. En el mismo directorio `custom`, cree el archivo `excludes.xml` con el contenido siguiente y especifique el nombre de clase a excluir dentro de la etiqueta `<exclude>`. Puede añadir tantas clases como sea necesario y el comodín asterisco (*) está soportado.

   ```
   <gpe>
     <bci>
       <classExcludes>
         <exclude>nombre_clase_a_excluir</exclude>
         <exclude>nombre_clase_a_excluir</exclude>
       </classExcludes>
     </bci>
   </gpe>
   ```

   Ejemplo:

   ```
   <gpe>
     <bci>
       <classExcludes>
         <exclude>org.apache.struts.action.ActionServlet</exclude>
         <exclude>com.company.package.*</exclude>
       </classExcludes>
     </bci>
   </gpe>
   ```
4. Reinicie el servidor de aplicaciones.

Qué hacer a continuación

Para verificar que la clase se ha excluido, busque en el archivo `toolkit.xml`. El nombre de clase debe aparecer en la sección `<classExcludes>`.

Recuerde: el archivo `toolkit.xml` contiene valores de tiempo de ejecución y se renueva cada vez que se reinicia el servidor de aplicaciones.

Personalización de correlación de información de solicitud

En algunos casos, es posible que tenga que cambiar la información que identifica las solicitudes supervisadas por el agente. Esta información incluye el nombre de solicitud y cualquier dato que pueda visualizarse para la solicitud (por ejemplo, el texto de consulta para una solicitud de SQL). Para cambiar la información, establezca una configuración de correlacionador de solicitudes personalizada.

Acerca de esta tarea

Para personalizar correlación de información de solicitud, debe definir una configuración de correlacionador de solicitudes personalizada en un archivo XML.

En este archivo, algunos *símbolos* incorporados representan valores del contexto de tiempo de ejecución de la solicitud. Puede crear símbolos adicionales, que calculen nuevos valores. El cálculo puede incluir valores de solicitud originales, expresiones, llamadas a métodos Java (incluidos métodos en la aplicación supervisada), condicionales e iteración de un conjunto de valores.

A continuación, puede *correlacionar* el contenido de los símbolos con los nuevos datos de solicitud que se proporcionan al Servidor de Cloud APM. Si no se correlaciona una variable particular en los datos de solicitud, se conserva el valor original.

Puesto que se recopilan datos distintos para tipos de solicitud, una configuración de correlacionador de solicitudes personalizada debe ser específica para un tipo de solicitud. Puede configurar distintos correlacionadores de solicitudes para distintos tipos de solicitud en el mismo recopilador de datos.

Procedimiento

Para establecer una configuración de correlacionador de solicitudes personalizada para un tipo de solicitud, complete los pasos siguientes:

1. Defina una configuración de correlacionador de solicitudes personalizada en un archivo XML.

   Para obtener información sobre la sintaxis de XML, consulte "Sintaxis de archivo XML" en la página 933.
2. Coloque el archivo XML en el directorio *dir_inicio_dc*/runtime/custom para utilizarlo para todas las instancias de servidor de aplicaciones o en el directorio *dir_inicio_dc*/runtime/*versión_servapl.nombre_nodo.nombre_perfil.nombre_servidor*/custom para utilizarlo para una instancia de servidor de aplicaciones.
3. Habilite la correlación de solicitudes personalizada para este tipo en el archivo de configuración personalizada del kit de herramientas, toolkit_custom.properties o toolkit_global_custom.properties.

   Para obtener instrucciones, consulte "Habilitación de un correlacionador de solicitudes" en la página 943.
4. Haga referencia al archivo XML que ha definido desde el mismo archivo de configuración personalizado del kit de herramientas.

   Para obtener instrucciones, consulte "Habilitación de un correlacionador de solicitudes" en la página 943.

Sintaxis de archivo XML

El archivo XML que crea para la configuración del correlacionador de solicitudes debe ser un XML válido y debe estar disponible cuando la configuración está en uso. Coloque el archivo XML en el directorio *dir_inicio_dc*/runtime/custom para utilizarlo para todas las instancias de servidor de aplicaciones o en el directorio *dir_inicio_dc*/runtime/*versión_servapl.nombre_nodo.nombre_perfil.nombre_servidor*/custom para utilizarlo para una instancia de servidor de aplicaciones.

Nivel superior

El código de nivel superior es <gpe>. Dentro de este código, utilice el código <runtimeConfiguration>. Estos códigos no tienen atributos.

Dentro del código <runtimeConfiguration>, cree un código <requestMapperDefinition>. Este código debe tener un atributo type. Establézcalo en el nombre de tipo del correlacionador de solicitudes para el tipo de solicitud requerido. Para obtener más información, consulte Tabla 233 en la página 945.

Dentro del código <requestMapperDefinition>, deben estar presentes los dos códigos siguientes:

<symbolDefinitions>
Contiene todas las definiciones de símbolos. Los símbolos representan valores que el agente calcula cada vez que se detecta una solicitud de este tipo.

<selection>
Contiene la correlación de claves de contexto con valores. Las claves representan los datos personalizados pasados al agente. Están predefinidos para cada tipo de solicitud. La correlación puede ser condicional.

Para obtener más información sobre propiedades de habilitación del correlacionador de solicitudes y nombres de tipo, consulte Tabla 233 en la página 945.

Además, dentro del código <runtimeConfiguration>, puede crear un código <requestMapperClassPath>. Dentro de este código, puede definir archivos JAR. Puede hacer referencia a clases Java en estos archivos JAR dentro de las definiciones del correlacionador de solicitudes.

Definición de una expresión
Para definir símbolos, debe utilizar expresiones. El agente evalúa las expresiones para asignar valores a los símbolos.

Uso de datos en una expresión
Una expresión puede utilizar los datos siguientes:

- Los símbolos de datos de entrada para el tipo de solicitud
- Otros símbolos descritos en la misma definición de correlacionador de solicitudes
- Constantes numéricas
- Constantes de tipo serie (delimitadas con ", por ejemplo, `"string"`)
- Constantes booleanas (`true`, `TRUE`, `false`, `FALSE`)
- La constante `null`

Para obtener más información acerca de los símbolos de datos de entrada, consulte Tabla 234 en la página 947.

Si el valor de un símbolo es una instanciación de una clase Java, las expresiones pueden contener referencias a campos y métodos definidos dentro de la clase. Para hacer referencia a un campo, utilice *symbol*`.`*fieldname*. Para hacer referencia a un método, utilice *symbol*`.`*methodname*`(`*parameters*`)`. La llamada a método debe devolver un valor. Por ejemplo, puede utilizar los métodos Java String con un símbolo que tenga un valor String.

Para hacer referencia a un campo estático o método de una clase, también puede utilizar *classname*`.`*fieldname* y *classname*`.`*methodname*`(`*parameters*`)`.

Si un símbolo hace referencia a un objeto de matriz, la expresión puede seleccionar un elemento (*symbol*`[`*selector*`]`) y determinar la longitud de la matriz (*symbol*`.length`)

Operadores

Puede utilizar los siguientes operadores en una expresión:

- Operadores booleanos: `AND`, `&`, `OR`, `|`, `NOT`, `!`
- Comparación: `==`, `!=`, `GT`, `>`, `LT`, `<`, `GE`, `>=`, `LE`, `<=`
- Operadores numéricos: `+`, `-`, `*`, `/`
- Paréntesis para forzar el orden de evaluación: `(`, `)`

Importante: Debe utilizar el carácter de escape con los símbolos <, >, y & en XML. De forma alternativa, puede utilizar los operadores `GT` (mayor que), `GE` (mayor que o igual a), `LT` (menor que), `LE` (menor que o igual a) y `AND`.

La expresión puede evaluar si un valor es una instancia de una clase, utilizando el operador `instanceof`:

```
expresión instanceof java.class.name
```

este operador, parecido al operador Java `instanceof`, genera una valor booleano. En este ejemplo, el valor es verdadero si la clase a la que pertenece el valor *expresión* cumple alguna de las condiciones siguientes:

- Se denomina *`java.class.name`*
- Es una subclase directa o indirecta de la clase identificada por *`java.class.name`*.
- Implementa, directa o indirectamente, la interfaz identificada por *`java.class.name`*.

La expresión también puede instanciar un nuevo objeto de una clase Java, utilizando el operador `new`. Este operador es parecido al operador Java `new`:

```
new java.class.name(expresión1, expresión2, ... expresiónN)
```

Prioridad de operador
Los operadores se evalúan en orden de prioridad. Los operadores del mismo orden de prioridad se evalúan de izquierda a derecha. Puede cambiar el orden de evaluación utilizando paréntesis `(` y `)`.

El orden de prioridad es el siguiente:

1. `.` operador (llamada a método o referencia de campo)
2. `[ ]` (selector de elemento de matriz)
3. `new`
4. `!`, `NOT`
5. `*`, `/`
6. `+`, `-`
7. `GT`, `>`, `LT`, `<`, `GE`, `>=`, `LE`, `<=`, `instanceof`
8. `==`, `!=`
9. `AND`, `&`
10. `OR`, `|`

Ejemplo

```
$s1 >= ( 2 * ($s2.sampMethod($s3, true) + 1))
```

El agente evalúa esta expresión de la forma siguiente:

1. Se evalúa el símbolo `$s1`. Debe producir un valor numérico.
2. Se evalúa el símbolo `$s2`. Debe producir un objeto Java.
3. Se evalúa el símbolo `$s3`.
4. Se llama a un método `sampMethod` para el objeto que resulta de la evaluación de `$s2`. El resultado de la evaluación de `$s3` se pasa como primer parámetro y el valor booleano `true` se pasa como segundo parámetro. La llamada a `sampMethod` debe devolver un valor numérico.
5. Se añade 1 al resultado del paso “4” en la página 935.
6. El resultado del paso “5” en la página 935 se multiplica por 2.
7. El resultado de paso “1” en la página 935 se compara con el del paso “6” en la página 935. Si el resultado del paso “1” en la página 935 es mayor o igual al resultado del paso “6” en la página 935, se devuelve `true`. De lo contrario, se devuelve `false`.

Definición de símbolos básicos
Para definir símbolos, debe utilizar expresiones. El agente evalúa las expresiones para asignar valores a los símbolos.

Dentro del código <symbol>, utilice los códigos siguientes:

<name>
El nombre del símbolo. Es una serie y debe empezar con el carácter $.

<eval>
La expresión que el agente debe evaluar para generar el valor para este símbolo. Para obtener más información sobre la definición de expresiones, consulte "Definición de una expresión" en la página 934.

<type>
El tipo del valor que devuelve el símbolo. Especifique este valor como un nombre de clase Java totalmente calificado o una primitiva Java. La especificación del tipo de símbolo es opcional. Si no se define, el correlacionador de solicitudes intenta establecer el tipo de campo según la expresión. Si el correlacionador de solicitudes no puede determinar el tipo de símbolo antes de evaluar la expresión, el rendimiento se ve afectado. Por tanto, para un rendimiento óptimo, es mejor especificar el tipo.

<args>
Los argumentos para el símbolo. Este código es opcional; si se especifica, deben proporcionarse argumentos para la evaluación del símbolo. Para obtener más información, consulte "Definición de argumentos de símbolo" en la página 936.

Ejemplo

```
<symbol>
   <name>$doubles1</name>
   <eval>$s1*2</eval>
   <type>int</type>
</symbol>
```

Este símbolo devuelve el doble del valor de otro símbolo, `$s1`.

Definición de argumentos de símbolo
Dentro de un código <args> de una definición de símbolo, puede definir tipos de argumentos para el símbolo.

En este código, utilice el código <type> para especificar los tipos de argumentos. Especifique este valor como un nombre de clase Java totalmente calificado o una primitiva Java. Puede especificar cualquier número de códigos <type>; cada uno de estos códigos define un argumento.

En este caso, debe hacerse referencia al símbolo con argumentos entre paréntesis:

```
$símbolo(argumento1,argumento2...)
```

El número de argumentos debe ser el mismo que el número de definiciones de tipo de argumento.

Dentro de la definición de símbolo, haga referencia al primer argumento como `$p0`, al segundo argumento como `$p1`, etc.

Un símbolo con argumentos funciona como un método Java. Toma argumentos de entrada y devuelve un valor que depende de los valores de los argumentos.

Ejemplo

```
<symbol>
   <name>$double</name>
   <eval>$p0*2</eval>
   <type>int</type>
   <args>
       <type>int</type>
   </args>
</symbol>
```

Este símbolo devuelve el doble del valor del argumento. Para evaluarlo, proporcione un argumento numérico: `$double(2)`, `$double($s1)`.

Definición de símbolos de iteración
Dentro del código <symbolDefinitions>, puede definir un símbolo de iteración utilizando el código <iterationSymbol>. Un símbolo de iteración representa un valor que se adquiere mediante la iteración a través de un conjunto de objetos en una matriz Java, enumeración o colección. Para cada uno de los miembros, el correlacionador de solicitudes evalúa una o más expresiones de condición. Si una expresión devuelve `true`, el correlacionador de solicitudes utiliza el miembro para calcular el valor de retorno. Cuando un miembro cumple la expresión de condición, el correlacionador de solicitudes no evalúa el resto de los miembros.

Dentro del código <iterationSymbol>, utilice los códigos siguientes.

<name>
El nombre del símbolo. Es una serie y debe empezar con el carácter $.

<type>
El tipo del valor que devuelve el símbolo. Especifique este valor como un nombre de clase Java totalmente calificado o una primitiva Java. La especificación del tipo de símbolo es opcional. Si no se define, el correlacionador de solicitudes intenta establecer el tipo de campo según la expresión. Si el correlacionador de solicitudes no puede determinar el tipo de símbolo antes de evaluar la expresión, el rendimiento se ve afectado. Por tanto, para un rendimiento óptimo, es mejor especificar el tipo.

<args>
Los argumentos para el símbolo. Este código es opcional; si se especifica, deben proporcionarse argumentos para la evaluación del símbolo. Para obtener más información, consulte "Definición de argumentos de símbolo" en la página 936.

<iterate over="*expresión*">
Define el objeto (matriz, enumeración o colección) que contiene los miembros en los que iterar. La expresión debe devolver un objeto así. El correlacionador de solicitudes itera en sus miembros hasta que uno de ellos hace que la expresión de condición devuelva `true`, o no queden más miembros. Defina el conjunto de expresiones de iteración en códigos dentro de este código:

<test>
Defina la condición y la expresión de devolución dentro de este código. Un código <iterate> puede contener varios códigos <test>. En este caso, el correlacionador de solicitudes los evalúa todos. Si una expresión de condición es verdadera, el símbolo devuelve un valor utilizando la expresión de resultado en el mismo código <test> y no se realizan más evaluaciones.

<castTo>
Opcional: Si este códigos está presente, especifique el nombre de un tipo Java dentro de él, como un nombre de clase Java totalmente calificado o una primitiva Java. El correlacionador de solicitudes convierte el elemento iterado a este tipo antes evaluar la condición y devolver expresiones. Si este código no está presente, el correlacionador de solicitudes convierte un miembro de una matriz al tipo base de matriz, y un miembro de una enumeración o colección en `java.lang.Object`. Para un miembro de matriz, el tipo base de matriz es normalmente la opción correcta; por tanto, utilice este código para que el correlacionador de solicitudes itere sobre una enumeración o colección.

<condition>
Una expresión que debe ofrecer un valor booleano. Utilice `$iterElement` para hacer referencia al elemento que se está iterando.

<return>
Si la expresión en el código <condition> devuelve `true`, el correlacionador de solicitudes evalúa la expresión en el código <return>. El símbolo de iteración devuelve el valor que genera esta expresión. Utilice `$iterElement` para hacer referencia al elemento que se está iterando.

<defaultValue>
Opcional. Si el correlacionador de solicitudes ha iterado sobre todos los miembros del objeto, pero ninguna expresión de condición ha devuelto `true`, el correlacionador de solicitudes evalúa la expresión en el código <defaultValue>. El símbolo de iteración devuelve el valor que genera la expresión. Si este código no está presente, el valor predeterminado es `null`.

Ejemplos

```
<iterationSymbol>
  <name>$userNameCookieValue</name>
  <iterate over="$httpServletRequest.getCookies()">
     <test>
        <condition>$iterElement.getName().equals("userName")</condition>
        <return>$iterElement.getValue()</return>
     </test>
   </iterate>
</iterationSymbol>
```

Este símbolo busca la cookie denominada "username" y devuelve su valor. `$httpServletRequest.getCookies()` devuelve una matriz, por lo que no es necesario el elemento <castTo>.

```
<iterationSymbol>
  <name>$headerNameStartingWithA</name>
  <iterate over="$httpServletRequest.getHeaderNames()">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.startsWith("A")</condition>
       <return>$iterElement</return>
    </test>
  </iterate>
</iterationSymbol>
```

Este símbolo busca la cabecera con un nombre que empieza por " A " y devuelve su nombre. `$httpServletRequest.getHeaderNames()` devuelve una enumeración, por lo que el elemento <castTo> es necesario.

```
<iterationSymbol>
  <name>$determined_gender</name>
  <iterate over="$children">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("male")</condition>
       <return>"It's a boy"</return>
    </test>
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("female")</condition>
       <return>"It's a girl"</return>
    </test>
  </iterate>
  <defaultValue>"unknown"</defaultValue>
</iterationSymbol>
```

Este símbolo itera en `$children`, que tiene que se una matriz, enumeración o colección de series. Si alguna de las series es igual a "male", devuelve "it's a boy". Si alguna de las series es igual a "female", devuelve "it's a girl". Finalmente, si ninguna serie en el objeto `$children` es igual a "male" o "female", el símbolo devuelve "unknown".

Definición de símbolos condicionales
Dentro del código <symbolDefinitions>, puede definir un símbolo condicional utilizando el código <conditionalSymbol>. Un símbolo condicional representa un valor que se adquiere mediante la evaluación de una serie de expresiones de condición. Si alguna expresión devuelve `true`, el correlacionador de solicitudes utiliza el miembro para calcular el valor de retorno. Cuando un miembro cumple la expresión de condición, el correlacionador de solicitudes evalúa una expresión de devolución correspondiente y devuelve el resultado. Una vez el correlacionador de solicitudes encuentra un resultado para devolver, no evalúa más expresiones.

Dentro del código <conditionalSymbol>, utilice los códigos siguientes.

<name>
El nombre del símbolo. Es una serie y debe empezar con el carácter $.

<type>
El tipo del valor que devuelve el símbolo. Especifique este valor como un nombre de clase Java totalmente calificado o una primitiva Java. La especificación del tipo de símbolo es opcional. Si no se define, el correlacionador de solicitudes intenta establecer el tipo de campo según la expresión. Si el correlacionador de solicitudes no puede determinar el tipo de símbolo antes de evaluar la expresión, el rendimiento se ve afectado. Por tanto, para un rendimiento óptimo, es mejor especificar el tipo.

<args>
Los argumentos para el símbolo. Este código es opcional; si se especifica, deben proporcionarse argumentos para la evaluación del símbolo. Para obtener más información, consulte "Definición de argumentos de símbolo" en la página 936.

<if condition="*expresión*">
El atributo `condition` define una expresión de condición a evaluar. La expresión debe ofrecer un valor booleano. Si el valor es `true`, el correlacionador de solicitudes utiliza el contenido del código <if> para intentar determinar el valor de retorno. El código <if> debe contener uno de los contenidos siguientes, pero no ambos:

- Un código <return>. Este código contiene una expresión. Si la expresión de condición es verdadera, el correlacionador de solicitudes evalúa la expresión y devuelve el resultado.
- Cualquier número de códigos <if>, anidados dentro de este código <if>. Si la expresión de condición es verdadera, el correlacionador de solicitudes procesa los códigos <if> anidados de la misma manera que un código <if> de nivel superior. Es decir, evalúa la expresión en el atributo `condition` y si la expresión es verdadera, utiliza el contenido del código para intentar determinar el valor de retorno.

Importante: Si se determina un valor de retorno, el correlacionador de solicitudes no evalúa más expresiones. Sin embargo, si una expresión de condición en un código <if> es verdadera, pero contiene códigos <if> anidados y ninguna de sus expresiones de condición es verdadera, no se determina ningún valor. En este caso, el correlacionador de solicitudes continúa evaluando las expresiones siguientes.

<defaultValue>
Opcional. Si el correlacionador de solicitudes ha evaluado todas las expresiones de condición, pero ninguna de ellas ha devuelto `true`, el correlacionador de solicitudes evalúa la expresión en el código <defaultValue>. El símbolo condicional devuelve el valor que genera la expresión. Si este código no está presente, el valor predeterminado es `null`.

Ejemplo

```
<symbol>
  <name>$GET</name>
  <eval>"GET"</eval>
</symbol>
<symbol>
  <name>$PUT</name>
  <eval>"PUT"</eval>
</symbol>
<conditionalSymbol>
  <name>$sessionAttribute</name>
  <if condition="$httpServletRequest.getSession(false) != null>
     <if condition="$httpServletRequest.getSession(false).getAttribute($GET)
!= null">
       <return>$httpServletRequest.getSession(false).getAttribute($GET)</return>
     </if>
     <if condition="true">
       <return>$httpServletRequest.getSession(false).getAttribute($PUT)</return>
      </if>
  </if>
</conditionalSymbol>
```

Se da por hecho que este símbolo forma parte del correlacionador de solicitudes de servlet. Primero, comprueba si existe una sesión HTTP para el servlet; si no, el símbolo devuelve `null`. Si existe una sesión, el símbolo comprueba si el servlet tiene un atributo GET, y devuelve el valor de ese atributo. De lo contrario, devuelve el valor del atributo PUT. La segunda expresión de condición es true; este valor se

utiliza como una cláusula else. Si la primera condición es true, el correlacionador de solicitudes no evalúa más expresiones; de lo contrario, continúa con la segunda expresión.

Definición de símbolos de clases externas
Dentro del código <symbolDefinitions>, puede definir una clase externa utilizando el código <externalClassSymbol>. Un símbolo de clase externa representa una clase Java externa. La definición de símbolo de clase externa es opcional; puede utilizar clases Java externas en expresiones directamente. Sin embargo, puede ampliar de legibilidad de la configuración del correlacionador de solicitudes.

Dentro del código <externalClassSymbol>, utilice los códigos siguientes.

<name>
El nombre del símbolo. Es una serie y debe empezar con el carácter $.

<className>
El nombre de la clase definida por el cliente.

Importante: Para hacer referencia a una clase Java en la configuración del correlacionador de solicitudes, tanto en una definición de símbolo de clase externa como en una expresión, debe añadir la vía de acceso completa y el nombre del archivo JAR que contiene la clase en el código <requestMapperClassPath> dentro del código <runtimeConfiguration>.

Después de definir un símbolo externo, puede hacer referencia a la clase por el nombre del símbolo. También puede hacer referencia a métodos estáticos y campos de la clase utilizando el símbolo.

Ejemplo

```
<externalClassSymbol>
  <name>$rand</name>
  <className>user.class.Random</className>
</externalClassSymbol>
```

Este símbolo hace referencia a una clase escrita por el usuario, que genera un número aleatorio. La vía de acceso completa y el nombre del archivo JAR que contiene esta clase deben estar presentes en el código <requestMapperClassPath> dentro del código <runtimeConfiguration>.

Para hacer referencia al método estático `user.class.Random.generate()` en una expresión, puede utilizar el símbolo externo:

```
$rand.generate()
```

Correlación de valores con claves de contexto
Dentro del código <requestMapperDefinition>, correlaciones valores con claves de contexto utilizando el código <selection>. Esta correlación proporciona los cambios en la información de supervisión.

Puede correlacionar valores con las claves de salida definidas para el tipo de solicitud. Para obtener más información, consulte Tabla 233 en la página 945.

Si no se correlaciona ningún valor con una clave después de la evaluación de la configuración del correlacionador de solicitudes, ITCAM utiliza el valor original extraído de la solicitud.

Dentro del código <selection>, utilice los códigos siguientes.

<matchCriteria>
Una expresión que debe devolver un valor booleano. La correlación definida dentro de este código solo se utiliza si esta expresión devuelve `true`.

<mapTo>
Define una clave y el valor para correlacionar. Dentro de este código, un código <key> contiene la clave y un código <value> contiene el valor.

<selection>
Puede anidar códigos <selection>, colocando uno dentro del otro.

Si los códigos <selection> están anidados, la correlación anidada solo se usa si ambas expresiones <matchCriteria>, la exterior y la anidada, devuelven `true`.

Puede utilizar varios códigos <selection> dentro de un código <requestMapperDefinition> o dentro de otro código <selection>. Si la misma clave se correlaciona varias veces en varios códigos <selection> (es decir, dentro del mismo código padre), se utiliza la primera correlación para la que la expresión <matchCriteria> devuelve `true`.

No correlacione la misma clave tanto en el código <selection> exterior como anidado.

Normalmente, utilice el valor de <matchCriteria> `true` como un valor "else" para el último código de selección en un nivel de anidamiento. Si desea correlacionar distintos valores en distintos casos, utilice varios códigos <selection> dentro de este código exterior; cada uno de ellos puede contener los criterios y valores para un caso particular. El último código, con un valor de `true`, cubre el caso cuando los datos disponibles no cumplen ninguno de los criterios.

Ejemplos

```
<selection>
   <matchCriteria>true</matchCriteria>
   <mapTo>
      <key>Result</key>
      <value>$s1</value>
   </mapTo>
</selection>
```

En esta configuración de correlación, `Result` se establece en el valor del símbolo `$s1`.

```
<matchCriteria>true</matchCriteria>
   <selection>
      <matchCriteria>$b1</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>1</value>
      </mapTo>
   </selection>
   <selection>
      <matchCriteria>true</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>2</value>
      </mapTo>
</selection>
```

En esta configuración de correlación, el símbolo $b1 debe devolver un valor booleano. `Result` se establece en 1 si $b1 devuelve `true`, y en 2 si $b1 devuelve `false`. Si $b1 devuelve `true`, el correlacionador de solicitudes utiliza la correlación para `Result` en el primer código <selection>; la correlación para la misma clave en el segundo código no se utiliza.

Definición de solicitudes personalizadas

De forma predeterminada, el recopilador de datos supervisa solo determinados tipos de clases y métodos Java como solicitudes. Servlets, JSP, métodos de negocio EJB y determinadas API Java EE estándar se reconocen como solicitudes. Puede designar clases y métodos adicionales como *solicitudes personalizadas*.

Acerca de esta tarea

Para habilitar la supervisión de solicitudes personalizadas por parte del recopilador de datos, defina las solicitudes personalizadas en un archivo XML y establezca la propiedad `am.camtoolkit.gpe.customxml.custom` en el archivo de propiedades personalizado del kit de herramientas.

Por ejemplo, de forma predeterminada el recopilador de datos no reconoce las clases de acción de Struts como solicitudes. No obstante, puede configurar definiciones de solicitudes personalizadas y hacer que las acciones se reconozcan como solicitudes anidadas.

Procedimiento

Realice el procedimiento siguiente para habilitar la supervisión de solicitudes personalizadas y designar uno o más métodos como solicitudes personalizadas:

1. Realice una copia del archivo *dir_inicio_dc*/itcamdc/etc/custom_requests.xml en una ubicación temporal. A continuación, abra la copia en un editor de texto.
2. Modifique los parámetros en el archivo.

   En la tabla siguiente se describen los parámetros que puede modificar:

Tabla 232. Parámetros del archivo de configuración de solicitudes personalizadas

Nombre de etiqueta	Descripción
edgeRequest	Identifica uno o más métodos de aplicaciones que deben instrumentarse mediante códigos de bytes para el proceso de solicitudes personalizadas. Modificando las etiquetas requestName, Matches, type y methodName de la etiqueta edgeRequest puede personalizar la selección. Cada etiqueta edgeRequest debe contener exactamente una etiqueta methodName y una o más etiquetas Matches. Se pueden especificar varias etiquetas edgeRequest.
requestName	Define un nombre exclusivo para esta solicitud. El nombre de solicitud se muestra al usuario cuando se rastrea la entrada y salida del método.
Matches	Identifica una o más clases que contengan los métodos que deben instrumentarse mediante códigos de bytes para el proceso de solicitudes personalizadas. Puede haber varias etiquetas Matches en una única etiqueta edgeRequest.
tipo	Indica si una clase debe ser una clase de sistema o aplicación para que coincida con la etiqueta edgeRequest.
methodName	Identifica los nombres de los métodos de una de las clases que identifica la etiqueta Matches que deben instrumentarse mediante códigos de bytes para el proceso de solicitudes personalizadas. Se puede especificar exactamente una etiqueta methodName en cada etiqueta edgeRequest.
requestMapper	Opcional. Si se especifica esta etiqueta, el recopilador de datos utiliza un correlacionador de solicitudes para determinar información que identifica la solicitud. Puede definir formas no estándar de extraer esta información. Para obtener más información sobre cómo habilitar y definir correlacionadores de solicitudes, consulte "Personalización de correlación de información de solicitud" en la página 932.

Recuerde: Las etiquetas Matches y methodName pueden incluir caracteres comodín. A continuación se describe el funcionamiento de los caracteres comodín:

- Un asterisco (*) representa una o más apariciones, o ninguna, de un carácter cualquiera cuando se interpreta como tal. Cuando se encuentra incorporado en una secuencia de caracteres (por ejemplo, java.*.String), coincide con cero o más ocurrencias de cualquier carácter, excepto el separador del paquete (.).
- Se puede utilizar dos puntos (..) para especificar todos los subpaquetes. Coincide con cualquier secuencia de caracteres que empieza y finaliza por el separador de paquetes (.). Por ejemplo, java..String coincide con java.lang.String e com.ibm..* coincide con cualquier declaración que empiece por com.ibm.

Por ejemplo, una aplicación con el nombre de paquete com.mycompany.myapp tiene los requisitos siguientes:

- En la clase Customer, el método creditCheck() se debe tratar como una solicitud personalizada denominada CreditCheck.
- En la clase Supplier, el método inventoryCheck() se debe tratar como una solicitud personalizada denominada SupplyCheck.

El contenido del archivo `custom_requests.xml` personalizado que cumple los requisitos es el siguiente:

```
<customEdgeRequests>
      <edgeRequest>
              <requestName>CreditCheck</requestName>
              <Matches>com.mycompany.myapp.Customer</Matches>
              <type>application</type>
              <methodName>creditCheck</methodName>
      </edgeRequest>
      <edgeRequest>
              <requestName>SupplyCheck</requestName>
              <Matches>com.mycompany.myapp.Supplier</Matches>
              <type>application</type>
              <methodName>inventoryCheck</methodName>
      </edgeRequest>
</customEdgeRequests>
```

3. Complete uno de los pasos siguientes:
   - Guarde el archivo en el directorio *dir_inicio_dc*/runtime/*versión_servidor_apl.nombre_nodo.nombre_perfil.nombre_servidor*/custom. A continuación, en el archivo de propiedades personalizadas del kit de herramientas, establezca la propiedad am.camtoolkit.gpe.customxml.custom en el nombre (sin vía de acceso) del archivo que ha modificado en el paso "2" en la página 942.
   - Guarde el archivo en cualquier directorio del sistema. A continuación, en el archivo de propiedades personalizadas del kit de herramientas, establezca la propiedad am.camtoolkit.gpe.customxml.custom en la vía de acceso y el nombre del archivo que ha modificado en el paso "2" en la página 942.

   Para obtener más información sobre el archivo de propiedades personalizadas del kit de herramientas, consulte "Archivo de propiedades del kit de herramientas" en la página 924.

Habilitación de un correlacionador de solicitudes

Para habilitar un correlacionador de solicitudes para una solicitud typeP, edite el archivo de configuración personalizado del kit de herramientas o el archivo de configuración personalizado global de kit de herramientas. Los procedimientos son distintos para tipos de solicitud comunes y para solicitudes personalizadas.

Antes de empezar

Defina la configuración del correlacionador de solicitudes en un archivo XML. A continuación, coloque el archivo XML que contiene la configuración del correlacionador de solicitudes en el mismo directorio que el archivo de propiedades del kit de herramientas.

- Para habilitar el correlacionador de solicitudes para todas las instancias de servidor de aplicaciones, colóquelo en el directorio *dir_inicio_dc*/runtime/custom.
- Para habilitar el correlacionador de solicitudes para una instancia de servidor de aplicaciones, colóquelo en el directorio *dir_inicio_dc*/runtime/*versión_servapl.nombre_nodo.nombre_perfil.nombre_servidor*/custom/.

Para obtener información sobre la sintaxis del archivo XML, consulte "Sintaxis de archivo XML" en la página 933.

Acerca de esta tarea

Edite el archivo `toolkit_custom.properties` o el archivo `toolkit_global_custom.properties` para habilitar el correlacionador de solicitudes para una o todas las instancias de servidor de aplicaciones.

Procedimiento

- Para habilitar un correlacionador de solicitudes para solicitudes comunes, complete los pasos siguientes:

a) En un editor de texto, abra uno de los siguientes archivos de configuración personalizados del kit de herramientas:

   – Para habilitar el correlacionador de solicitudes para todas las instancias de servidor de aplicaciones, abra el archivo *dir_inicio_dc*/runtime/custom/toolkit_global_custom.properties.

   – Para habilitar el correlacionador de solicitudes para una instancia de servidor de aplicaciones, abra el archivo *dir_inicio_dc*/runtime/*versión_servapl.nombre_nodo.nombre_perfil.nombre_servidor*/custom/toolkit_custom.properties/.

b) Edite el archivo de propiedades del kit de herramientas de la manera siguiente:

   – Añada una línea que establezca la propiedad de habilitación para este tipo de solicitud en `true`. Para obtener más información, consulte el apartado Tabla 233 en la página 945.

   – Añada una línea que establezca la propiedad `am.camtoolkit.gpe.customxml.*` en el nombre del archivo XML del correlacionador. Utilice cualquier valor exclusivo en lugar del símbolo *. Para obtener más información, consulte "Sintaxis de archivo XML" en la página 933.

c) Guarde y cierre el archivo de propiedades.

Ejemplo:

Para habilitar un correlacionador de solicitudes que está definido en `renameDataSource.xml` para el tipo de solicitud SQL, añada las líneas siguientes en el archivo de configuración personalizado del kit de herramientas o el archivo de configuración personalizado global del kit de herramientas:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

- Para habilitar un correlacionador de solicitudes para solicitudes personalizadas, complete los pasos siguientes:

  a) Bajo el código <edgerequest> en el archivo XML de definición de solicitudes personalizadas, cree un código <requestMapper>. Coloque un nombre de tipo de correlación de solicitud exclusivo en este código. Para obtener más información sobre la definición de solicitudes personalizadas, consulte "Definición de solicitudes personalizadas" en la página 941.

  b) En el archivo XML del correlacionador de solicitudes, utilice el nombre de tipo de correlación de solicitud exclusivo en el atributo `type` del código <requestMapperDefinition>.

  c) En un editor de texto, abra uno de los siguientes archivos de configuración personalizados del kit de herramientas:

     – Para habilitar el correlacionador de solicitudes para todas las instancias de servidor de aplicaciones, abra el archivo *dir_inicio_dc*/runtime/custom/toolkit_global_custom.properties.

     – Para habilitar el correlacionador de solicitudes para una instancia de servidor de aplicaciones, abra el archivo *dir_inicio_dc*/runtime/*versión_servapl.nombre_nodo.nombre_perfil.nombre_servidor*/custom/toolkit_custom.properties/.

  d) Edite el archivo de propiedades del kit de herramientas para añadir una línea que establezca la propiedad `am.camtoolkit.gpe.customxml.*` en el nombre del archivo XML del correlacionador. Utilice cualquier valor exclusivo en lugar del símbolo *. Para obtener más información, consulte "Sintaxis de archivo XML" en la página 933.

  e) Guarde y cierre el archivo de propiedades.

  Ejemplo:

  Para habilitar un correlacionador de solicitudes que está definido en `customMapper.xml` para el tipo de solicitud personalizado `SupplyCheck` definido en el archivo `custom_requests.xml`, complete los pasos siguientes:

1. Utilice la definición siguiente en el archivo `custom_requests.xml`:

```
<customEdgeRequests>
  <edgeRequest>
    <requestName>SupplyCheck</requestName>
    <Matches>com.mycompany.myapp.Supplier</Matches>
    <type>application</type
    <methodName>inventoryCheck</methodName>
    <requestMapper>customMapper</requestMapper>
  </edgeRequest>
</customEdgeRequests>
```

2. En el archivo `customMapper.xml`, asegúrese de que se establece el nombre de tipo:

```
<requestMapperDefinition type="customMapper">
```

3. Añada la línea siguiente en el archivo de configuración personalizado del kit de herramientas o el archivo de configuración personalizado global del kit de herramientas:

```
am.camtoolkit.gpe.customxml.customMapper=customMapper.xml
```

Nombres de tipo, datos de entrada y de salida del correlacionador de solicitudes
Las tablas siguientes listan la información necesaria para configurar y habilitar correlacionadores para distintos tipos de solicitud.

El significado de cada cabecera de tabla es el siguiente:

Tipo de solicitud
El tipo de solicitud.

Propiedad de habilitación
Para habilitar el correlacionador de solicitudes, establezca esta propiedad en `true` en el archivo `toolkit_custom.properties` o `toolkit_global_custom.properties`.

Importante: Si copia este valor de la tabla, elimine cualquier espacio y salto de línea.

Nombre de tipo de correlacionador de solicitudes
Asigne este valor al atributo `type` del código <requestMapperDefinition> en el archivo XML de definición de correlacionador de solicitudes.

Nombres de símbolo de datos de entrada
Los símbolos que representan la información de la solicitud. Puede utilizar estos símbolos en expresiones dentro de las definiciones de correlacionador de solicitudes. Para obtener más información, consulte "Definición de una expresión" en la página 934.

Claves de contexto de datos de salida
Para proporcionar cambios en la información de supervisión, asigne valores a estas claves en la definición de correlacionador de solicitudes. Para obtener más información, consulte "Correlación de valores con claves de contexto" en la página 940.

Tabla 233. Propiedades de habilitación de correlacionador de solicitudes y nombres de tipo

Tipo de solicitud	Propiedad de habilitación	Nombre de tipo de correlacionador de solicitudes
Servlet	`com.ibm.tivoli.itcam.toolkit.ai.enable.servletrequestmapper`	`servlet`
JNDI	`com.ibm.tivoli.itcam.toolkit.ai.enable.jndirequestmapper`	`jndiLookup`
Solicitud personalizada		Definida por el usuario en la definición edgeRequest

Tabla 233. Propiedades de habilitación de correlacionador de solicitudes y nombres de tipo (continuación)

Tipo de solicitud	Propiedad de habilitación	Nombre de tipo de correlacionador de solicitudes
EJB	com.ibm.tivoli.itcam.toolkit.ai.enable.ejbrequestmapper	ejb
JCA	com.ibm.tivoli.itcam.toolkit.ai.enable.jcarequestmapper	jca
Origen de datos JDBC	com.ibm.tivoli.itcam.toolkit.ai.enable.datasourcerequestmapper	dataSource
Sentencia SQL JDBC	com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper	sqlStatement
JMS	com.ibm.tivoli.itcam.toolkit.ai.enable.jmsrequestmapper	jms
Servicio web JAX-RPC	com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper	webServices
Servicio web de Axis	com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper	webServices
MQI	com.ibm.tivoli.itcam.toolkit.ai.enable.mqrequestmapper	mqi
EJB	com.ibm.tivoli.itcam.toolkit.ai.enable.ejbrequestmapper	ejb
Fábrica de conexiones JDBC	com.ibm.tivoli.itcam.toolkit.ai.enable.sqlconnectfactoryrequestmapper	connectionFactory
SCA	com.ibm.tivoli.itcam.toolkit.ai.enable.scarequestmapper	sca
Servicio web JAX-WS	com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper	webServices
Portal de WebSphere Portal Server (ampliando la clase org.apache.jetspeed.portlet.Portlet)	com.ibm.tivoli.itcam.toolkit.ai.enable.portalrequestmapper	portalPortal
Portal de WebSphere Portal Server versión 6.1, 7 y 8 (implementa la interfaz javax.portlet.Portlet)	com.ibm.tivoli.itcam.toolkit.ai.enable.portal6requestmapper	Portal6Portal

Importante: No hay una manera significativa de configurar el correlacionador de solicitudes personalizado para los tipos de solicitud que no se listan en Tabla 233 en la página 945.

Tabla 234. Datos de entrada y salida del correlacionador de solicitudes

Tipo de solicitud	Nombres de símbolo de datos de entrada	Claves de contexto de datos de salida
Servlet	Para obtener más información, consulte Tabla 235 en la página 951.	**remappedURI** define un URI renombrado **remappedURL** define un URL renombrado **appName** define un nombre de aplicación renombrada **userid** define el ID de usuario de la solicitud
JNDI	• **$jndiContext** el objeto de Contexto • **$lookup** la serie de búsqueda • **$context** "JNDIlookup"	**renamedLookup** define una serie de búsqueda renombrada
Solicitud personalizada	• **$this** el objeto 'this' para el método de solicitud personalizada • **$0** los argumentos pasados al método de solicitud personalizada, especificados como una matriz de objetos • **$className** el nombre de clase de la solicitud personalizada • **$methodName** el nombre de método de la solicitud personalizada • **$context** el nombre de solicitud original de la definición de edgeRequest	**customRequestName** define el nombre de solicitud personalizada renombrado
EJB	• **$ejb** el objeto de implementación EJB • **$appName** el nombre de la aplicación • **$ejbType** el tipo de EJB • **$className** el nombre de clase del objeto de implementación EJB • **$methodName** el nombre de método de negocio EJB • **$context** "EJBBusinessMethod"	**appName** define el nombre de aplicación renombrada **ejbType** define el tipo de EJB renombrado **className** define el nombre de clase renombrado **methodName** define el nombre de método renombrado
JCA	• **$interaction** el objeto Interaction • **$interactionSpec** el objeto InteractionSpec • **$record** el objeto Record • **$context** "J2Cexecute"	**lookupName** es el lookupName renombrado **productName** es el nombre de producto renombrado **productVersion** es la versión del producto renombrado

Tabla 234. Datos de entrada y salida del correlacionador de solicitudes (continuación)

Tipo de solicitud	Nombres de símbolo de datos de entrada	Claves de contexto de datos de salida
Origen de datos JDBC	• **$this** el origen de datos o el objeto controlador • **$dataSource** el objeto $this, convertido en origen de datos • **$driver** el objeto $this, convertido en controlador • **$dataSourceName** es el nombre del origen de datos, como java.lang.String • **$context** indica el tipo de solicitud, "JDBCgetConnection" o "JDBCgetConnection FromDriver"	**dataSourceName** es el nombre de origen de datos renombrado, si el objeto $this es un origen de datos **url** es el URL de controlador renombrado, si el objeto $this es un controlador
Sentencia SQL JDBC	• **$this** la sentencia SQL o la conexión SQL • **$sqlText** contiene el texto SQL como java.lang.String, si el objeto $this es una sentencia SQL • **$sqlStatement** el objeto $this, convertido en sentencia SQL • **$sqlConnection** el objeto $this, convertido en conexión SQL • **$dataSourceName** el nombre de origen de datos • **$context** indica el tipo de solicitud: "JDBCexecute", JDBCexecuteQuery", "JDBCexecuteUpdate", "JDBCcreateStatement", "JDBCprepareStatement"	**dataSourceName** es el nombre de origen de datos renombrado **sqlText** es el texto SQL renombrado

Tabla 234. Datos de entrada y salida del correlacionador de solicitudes (continuación)

Tipo de solicitud	Nombres de símbolo de datos de entrada	Claves de contexto de datos de salida
JMS	• **$this** el objeto 'this' para el método instrumentado. Puede ser un QueueBrowser, MessageConsumer, MessageProducer o MessageListener • **$0** el objeto Queue, para una solicitud de envío, o un objeto de tema, para una solicitud Publish • **$queueBrowser** el objeto $this, convertido en un QueueBrowser • **$messageConsumer** el objeto $this, convertido en un MessageConsumer • **$messageProducer** el objeto $this, convertido en un MessageProducer • **$messageListener** el objeto $this, convertido en un MessageListener • **$queue** el objeto $0, convertido en una cola • **$topic** el objeto $0, convertido en un tema • **$context** indica el tipo de solicitud: "JMSreceive", "JMSsend", "JMSbrowse", "JMSpublish", "JMSonmessage"	**queueName** el nombre de cola renombrado **providerURL** el URL de proveedor renombrado **topicName** el nombre de tema renombrado
Servicio web JAX-RPC	• **$messageContext** el IMessageContextWrapper • **$appName** el nombre de aplicación • **$requestName** el nombre de solicitud predeterminado • **$url** el URL • **$context** indica el tipo de solicitud: "WebServicesJaxRpc ProviderRequest", "WebServicesJaxRpc ClientRequest"	**appName** el nombre de aplicación renombrada **requestName** el nombre de solicitud renombrada **url** el URL renombrado
Servicio web de Axis	• **$messageContext** el IMessageContextWrapper • **$appName** el nombre de aplicación • **$requestName** el nombre de solicitud predeterminado • **$url** el URL • **$context** indica el tipo de solicitud: "WebServicesAxisClient Request", "WebServicesAxis ProviderRequest"	**appName** el nombre de aplicación renombrada **requestName** el nombre de solicitud renombrada **url** el URL renombrado

Tabla 234. Datos de entrada y salida del correlacionador de solicitudes (continuación)

Tipo de solicitud	Nombres de símbolo de datos de entrada	Claves de contexto de datos de salida
MQI	• **$queue** el objeto MQQueue, si es conocido • **$qmgr** el objeto MQQueueManager, si es conocido • **$message** el objeto MQMessage o MQMsg2, si es conocido • **$session** el objeto MQSESSION, si es conocido • **$getMsgOptions** el objeto MQGetMessageOptions, si es conocido • **$qmgrName** el nombre del gestor de colas • **$queueName** el nombre de la cola • **$context** indica el tipo de solicitud MQ: "MQCONN", "MQCONNX", "MQDISC", "MQBACK", "MQBEGIN", "MQCLOSE", "MQCMIT", "MQINQ", "MQOPEN", "MQSET", "MQGET", "MQPUT", "MQPUT1", "MQGETBROWSE"	**qmgrName** el nombre de gestor de colas renombrado **qname** el nombre de cola renombrado
EJB	• **$appName** el nombre de la aplicación • **$ejbType** el tipo de EJB • **$className** el nombre de clase del objeto de implementación EJB • **$methodName** el nombre de método de negocio EJB • **$context** "EJBBusinessMethod"	**appName** define el nombre de aplicación renombrada **ejbType** define el tipo de EJB renombrado **className** define el nombre de clase renombrado **methodName** define el nombre de método renombrado
Fábrica de conexiones JDBC	• **$connectionFactory** la ConnectionFactory • **$dataSourceName** el nombre de origen de datos • **$context** "JDBCgetConnection"	**dataSourceName** es el nombre de origen de datos renombrado
SCA	• **$uri** el URI • **$operationName** el nombre de operación • **$context** indica el tipo de solicitud: "SCA_Generic", "SCA_Ref", "SCA_Target"	**uri** es el URI renombrado **operationName** es el nombre de operación renombrado

Tabla 234. Datos de entrada y salida del correlacionador de solicitudes (continuación)		
Tipo de solicitud	**Nombres de símbolo de datos de entrada**	**Claves de contexto de datos de salida**
Servicio web JAX-WS	• **$messageContext** el IMessageContextWrapper • **$appName** el nombre de aplicación • **$requestName** el nombre de solicitud predeterminado • **$url** el URL • **$context** indica el tipo de solicitud: "WebServicesJAXWS ClientRequest", "WebServicesJAXWS ProviderRequest", "WebServicesJAXWS AsyncRequest"	**appName** el nombre de aplicación renombrada **requestName** el nombre de solicitud renombrada **url** el URL renombrado
Portal de WebSphere Portal Server (ampliando la clase `org.apache.jetspeed.portlet.Portlet`)	• **$portletAdapter** PortletAdapter • **$portletRequest** PortletRequest • **$portletResponse** PortletResponse • **$portletName** nombre de Portlet • **$pageTitle** título de página • **$url** URL de la solicitud • **$userid** ID de usuario de solicitud • **$context** "Portal.Portlet"	**portletName** el nombre de portlet renombrado **title** el título de página renombrado **url** el URL renombrado **userid** el ID de usuario renombrado
Portal de WebSphere Portal Server versión 6.1, 7 y 8 (implementando la interfaz `javax.portlet.Portlet`)	• **$portlet** Portlet • **$renderRequest** RenderRequest • **$renderResponse** RenderResponse • **$portletName** nombre de Portlet • **$pageTitle** título de página • **$url** URL de la solicitud • **$userid** ID de usuario de solicitud • **$context** "Portal.Portlet"	**portletName** El nombre de portlet renombrado **title** El título de página renombrado **url** El URL renombrado **userid** El ID de usuario renombrado

Para solicitudes de servlet, se proporciona un gran número de símbolos de datos de entrada.

Tabla 235. Nombres de símbolo de datos de entrada para solicitudes de servlet		
Nombre de símbolo	**Tipo de valor**	**Contenido de símbolo**
$context	Serie	"ServletMethod"
$servlet	javax.servlet.http.HttpServlet	El objeto HttpServlet asociado con la solicitud de servlet
$httpServletRequest	javax.servlet.http.HttpServletRequest	El objeto HttpServletRequest asociado con la solicitud de servlet
$httpServletResponse	javax.servlet.http.HttpServletResponse	El objeto HttpServletResponse asociado con la solicitud de servlet
$appName	java.lang.String	El nombre de aplicación asociado con el servlet

Tabla 235. Nombres de símbolo de datos de entrada para solicitudes de servlet (continuación)		
Nombre de símbolo	**Tipo de valor**	**Contenido de símbolo**
$URL	java.lang.StringBuffer	El URL que el cliente ha utilizado para hacer la solicitud
$RemoteUser	java.lang.String	El nombre de inicio de sesión del usuario que hace la solicitud, si autenticado
$URI	java.lang.String	La parte del URL de solicitud del nombre de protocolo hasta la serie de consulta
$ServletPath	java.lang.String	La parte del URL de solicitud que llama al servlet.
$SessionID	javax.servlet.http.HttpSession	La sesión actual asociada con esta solicitud
$QueryString	java.lang.String	La serie de consulta contenida en el URL de solicitud después de la vía de acceso.
$SessionAttribute	java.lang.String	Este símbolo parametrizado devuelve un valor de atributo de sesión. Tiene un parámetro, el nombre de atributo (debe ser una serie). Por ejemplo, `$SessionAttribute ("attr1")` devuelve el valor del atributo denominado attr1.
$cookie	javax.servlet.http.Cookie	Este símbolo parametrizado devuelve una cookie con nombre. Tiene un parámetro, el nombre de cookie (debe ser una serie). Por ejemplo, `$cookie ("cookie1")` devuelve el valor del atributo denominado cookie1.

Definiciones de ejemplo del correlacionador de solicitudes
Los siguientes ejemplos ilustran el uso de la funcionalidad del correlacionador de solicitudes.

Cambio del nombre de aplicación de servlet
En este ejemplo, el nombre de aplicación en una solicitud de servlet se sustituye por el URI y la serie de consulta.

El archivo *dir_inicio_dc*`/runtime/changeAppname.xml` contiene la definición de correlacionador de solicitudes siguiente:

```
<gpe>
   <runtimeConfiguration>
         <requestMapperDefinition type="servlet">
               <selection>
                     <matchCriteria>true</matchCriteria>
                     <mapTo>
                           <key>appName</key>
                           <value>$URI + “.” + $QueryString</value>
                     </mapTo>
               </selection>
         </requestMapperDefinition>
```

```
   </runtimeConfiguration>
</gpe>
```

Cambio de nombre de un origen de datos
En este ejemplo, se cambia el nombre de origen de datos en una solicitud SQL a una versión que el usuario puede comprender más fácilmente.

El archivo *dir_inicio_dc*/runtime/renameDataSource.xml contiene la definición de correlacionador de solicitudes siguiente:

```
<gpe>
 <runtimeConfiguration>
   <requestMapperDefinition type=”sqlStatement”>
      <selection>
         <matchCriteria>$dataSourceName != null</matchCriteria>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/TradeDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Daytrader Data Source"</value>
           </mapTo>
         </selection>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/LongDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Long term trader Data Source"</value>
           </mapTo>
         </selection>
      </selection>
   </requestMapperDefinition>
 </runtimeConfiguration>
<gpe>
```

El primer código <selection> asegura que $dataSourceName no es nulo. A continuación, el segundo código <selection> puede evaluar de forma segura $dataSourceName.equals().

Si el primer código <selection> no estuviera presente y se hubiera pasado un $dataSourceName nulo, el correlacionador de solicitudes generaría una excepción. Una excepción así podría implicar la pérdida de información de supervisión.

Para habilitar este correlacionador de solicitudes, el archivo *dir_inicio_dc*/runtime/toolkit_global_custom.properties contiene las líneas siguientes:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

Supresión de información confidencial de una solicitud SQL
En este ejemplo, una aplicación incluye números de seguridad social en solicitudes SQL. El correlacionador de solicitudes elimina los números de la versión de la solicitud que puede ver el usuario.

En las solicitudes SQL, el número de la seguridad social se lista con el nombre de columna SS, SS = *número*. El correlacionador de solicitudes busca la serie SS = y elimina los nueve símbolos detrás de ella.

El archivo *dir_inicio_dc*/runtime/removeSSN.xml contiene la definición de correlacionador de solicitudes siguiente:

```
<gpe>
    <runtimeConfiguration>
         <requestMapperDefinition type="sqlStatement">
             <symbolDefinitions>
                 <symbol>
                     <name>$offsetOfSS</name>
                     <eval>$sqlText.indexOf("SS = ")</eval>
                 </symbol>
                 <symbol>
                     <name>$sqlTextContainsSS</name>
<eval>$sqlText != null AND $offsetOfSS > 0 AND $sqlText.length() GE
```

```
$offsetOfSS+16</eval>
                </symbol>
                <conditionalSymbol>
                    <name>$sqlTextPriorToSSKeyword</name>
                    <type>java.lang.String</type>
                    <defaultValue>""</defaultValue>
                    <if condition="$sqlTextContainsSS">
                      <return>$sqlText.substring(0, $offsetOfSS+5)</return>
                    </if>
                </conditionalSymbol>
                <conditionalSymbol>
                    <name>$sqlTextAfterSS</name>
                    <type>java.lang.String</type>
                    <defaultValue>""</defaultValue>
                    <if condition="$sqlTextContainsSS">
                      <return>$sqlText.substring($offsetOfSS+16)</return>
                    </if>
                </conditionalSymbol>
            </symbolDefinitions>
            <selection>
                 <matchCriteria>$sqlText != null AND $sqlText.length() >
0</matchCriteria>
                  <selection>
                       <matchCriteria>$sqlTextContainsSS</matchCriteria>
                       <mapTo>
                            <key>sqlText</key>
                            <value>$sqlTextPriorToSSKeyword + "?" +
$sqlTextAfterSS</value>
                       </mapTo>
                  </selection>
            </selection>
        </requestMapperDefinition>
    </runtimeConfiguration>
</gpe>
```

Para habilitar este correlacionador de solicitudes, el archivo *dir_inicio_dc*/runtime/toolkit_global_custom.properties contiene las líneas siguientes:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=removeSSN.xml
```

Configuración del Agente de WebSphere Applications para supervisar WebSphere Extreme Scale

Después de instalar el Agente de WebSphere Applications, puede realizar una configuración adicional para supervisar WebSphere Extreme Scale (WXS) en un entorno autónomo o de WebSphere Application Server.

Acerca de esta tarea

Los pasos de configuración son distintos en función de la modalidad de instalación de WebSphere Extreme Scale y de si la seguridad está habilitada. Siga estos pasos antes de ejecutar el proceso de configuración.

Procedimiento

1. Confirme la modalidad de instalación de WebSphere Extreme Scale.

   Modalidad autónoma
   WebSphere Extreme Scale se instala en un entorno que no tiene WebSphere Application Server.

   Modalidad WAS incorporado
   WebSphere Extreme Scale se instala en un entorno WebSphere Application Server.
2. Confirme si la seguridad está habilitada para WebSphere Extreme Scale. Si se utiliza un cliente Java™ seguro en modalidad de WebSphere Application Server incorporado, debe realizar unos pasos de conexión de seguridad.
3. Pulse los enlaces para obtener instrucciones.

   - Para configurar WebSphere Extreme Scale en un entorno autónomo, pulse "Configuración de la supervisión de WebSphere Extreme Scale en un entorno autónomo" en la página 955.

- Para configurar WebSphere Extreme Scale en un entorno incorporado sin seguridad, pulse "Configuración de la supervisión de WebSphere Extreme Scale en el entorno de WebSphere sin la seguridad habilitada" en la página 956.
- Para configurar WebSphere Extreme Scale en un entorno incorporado con la seguridad habilitada, pulse "Configuración de la supervisión de WebSphere Extreme Scale en un entorno de WebSphere habilitado para la seguridad" en la página 957.

Configuración de la supervisión de WebSphere Extreme Scale en un entorno autónomo
Aprenda a configurar el Agente de WebSphere Applications cuando WebSphere Extreme Scale se ha instalado en un entorno que no tiene WebSphere Application Server.

Procedimiento

1. Detenga el Agente de WebSphere Applications.
   a) Vaya al directorio *dir_instalación* donde se instala el Agente de WebSphere Applications.
   b) Ejecute el mandato `bin/was-agent.sh stop`.
2. Ejecute el script de configuración.

   ```
   dir_instalación/código_plataforma/yn/bin/wxs-agent-config.sh config
   ```

   Donde
   - *dir_instalación* es el directorio de instalación de Agente de WebSphere Applications.
   - *código_plataforma* es el código de la plataforma en el que se instala el agente, por ejemplo, lx8266 representa Linux x86_64 R2.6 (64 bits), aix536 representa AIX R5.3 (64 bits).

   Mandato de ejemplo:

   ```
   /opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh config
   ```

   ```
   /opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh config
   ```
3. Cuando se le solicite la vía de acceso de instalación del agente, especifique el directorio de inicio del Agente de WebSphere Applications.

   Nota: El script busca el nombre del archivo de configuración en función de la vía de acceso de instalación que especifique. El valor predeterminado es *dir_instalación*`/config/${hostname}_yn.xml`. Si se le indica que el archivo no existe, podría deberse a que no se ha iniciado el Agente de WebSphere Applications antes de realizar esta configuración. Inicie el Agente de WebSphere Applications y deténgalo al menos una vez.
4. Cuando se le solicite el `Tipo de conector del servidor de catálogo de WebSphere Extreme Scale`, especifique 1 para continuar.
5. Cuando se le solicite `Especificar un nombre de nodo para identificar este nodo de agente en la IU`, especifique el nombre de nodo.

   El nombre de nodo se utiliza para identificar la zona de WebSphere Extreme Scale supervisada y se visualiza en el nombre de instancia que puede ver en la interfaz de usuario del Panel de instrumentos de Rendimiento de aplicaciones.
6. Cuando se le solicite `¿Seguridad de servidor de catálogo de WebSphere Extreme Scale habilitada?`, especifique 1 si la seguridad está habilitada. A continuación, especifique el nombre de usuario y la contraseña. Si no hay seguridad habilitada, especifique 2.
7. Especifique el nombre de host y el número de puerto del servidor de catálogo. Si hay varios servidores de catálogo, puede añadirlos de uno en uno. También puede añadir varias zonas una tras otra.
   - El nombre de host es el nombre del sistema donde está ubicado el servidor de catálogo. Asegúrese de que se puede acceder al nombre de host. De lo contrario, utilice la dirección IP como nombre de host.

- El número de puerto es el número **JMXServicePort** del servidor de catálogo de WebSphere Extreme Scale. El valor por omisión es 1099. Se pueden encontrar más detalles sobre el número de puerto en WebSphere Extreme Scale Knowledge Center.

8. Para iniciar el agente, ejecute el mandato siguiente.

```
dir_instalación/bin/was-agent.sh start
```

Nota:

- La configuración del agente se almacena en *dir_instalación*/config/${hostname}_yn.xml. Si desea cambiar cualquier configuración, ejecute este script de nuevo o modifique el archivo .xml directamente.
- Se hace una copia de seguridad de la configuración anterior como *dir_instalación*/config/${hostname}_yn.xml.bak. Puede restaurar la configuración anterior si es necesario.
- Puede pulsar Ctrl-C para salir del script cuando ejecute *dir_instalación*/*código_plataforma*/yn/bin/wxs-agent-config.sh config. La configuración existente no se cambia.

Configuración de la supervisión de WebSphere Extreme Scale en el entorno de WebSphere incorporado

Aprenda a configurar el Agente de WebSphere Applications cuando WebSphere Extreme Scale está instalado en un entorno de WebSphere Application Server.

Acerca de esta tarea

Si la seguridad no está habilitada para el servidor de WebSphere Extreme Scale, puede ejecutar directamente el proceso de configuración. De lo contrario, primero debe completar el procedimiento "Configuración de la supervisión de WebSphere Extreme Scale en un entorno de WebSphere habilitado para la seguridad" en la página 957.

Configuración de la supervisión de WebSphere Extreme Scale en el entorno de WebSphere sin la seguridad habilitada

Si instala WebSphere Extreme Scale en un entorno de WebSphere Application Server sin la seguridad habilitada, puede configurar directamente el Agente de WebSphere Applications.

Procedimiento

1. Detenga Agente de WebSphere Applications.
   a) Vaya al directorio *dir_instalación* donde se instala el Agente de WebSphere Applications.
   b) Ejecute el mandato bin/was-agent.sh stop.
2. Ejecute el script de configuración.

```
dir_instalación/código_plataforma/yn/bin/wxs-agent-config.sh
config
```

   Donde

   - *dir_instalación* es el directorio de instalación de Agente de WebSphere Applications.
   - *código_plataforma* es el código de la plataforma en el que se instala el agente, por ejemplo, lx8266 representa Linux x86_64 R2.6 (64 bits), aix536 representa AIX R5.3 (64 bits).

   Mandato de ejemplo:

```
/opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh
```

```
/opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh
```

3. Cuando se le solicite la vía de acceso de instalación del agente, especifique el directorio de inicio del Agente de WebSphere Applications.

Nota: El script busca el nombre del archivo de configuración en función de la vía de acceso de instalación que especifique. El valor predeterminado es *dir_instalación*/config/${hostname}_yn.xml. Si se le indica que el archivo no existe, podría deberse a que no se ha iniciado el Agente de WebSphere Applications antes de realizar esta configuración. Inicie el Agente de WebSphere Applications y deténgalo al menos una vez.

4. Cuando se le solicite el Tipo de conector del servidor de catálogo de WebSphere Extreme Scale, especifique 2 para continuar.
5. Cuando se le solicite Especificar un nombre de nodo para identificar este nodo de agente en la IU, especifique el nombre de nodo.

   El nombre de nodo se utiliza para identificar la zona de WebSphere Extreme Scale supervisada y se visualiza en el nombre de instancia que puede ver en la interfaz de usuario del Panel de instrumentos de Rendimiento de aplicaciones.
6. Cuando se le solicite ¿Seguridad de servidor de catálogo de WebSphere Extreme Scale habilitada?, especifique 2 para continuar.
7. Especifique el nombre de host y el número de puerto del servidor de catálogo. Si hay varios servidores de catálogo, puede añadirlos de uno en uno. También puede añadir varias zonas una tras otra.
   - El nombre de host es el nombre del sistema donde está ubicado el servidor de catálogo. Asegúrese de que se puede acceder al nombre de host. De lo contrario, utilice la dirección IP como nombre de host.
   - El número de puerto indica el número **JMXServicePort** del servidor de catálogo de WebSphere Extreme Scale. Se hereda del valor de **BOOTSTRAP_ADDRESS** para cada WebSphere Application Server. Se pueden encontrar más detalles sobre el número de puerto en WebSphere Extreme Scale Knowledge Center.
8. Para iniciar el agente, ejecute el mandato siguiente.

   ```
   dir_instalación/bin/was-agent.sh start
   ```

   Nota:
   - La configuración del agente se almacena en *dir_instalación*/config/${hostname}_yn.xml. Si desea cambiar cualquier configuración, ejecute este script de nuevo o modifique el archivo .xml directamente.
   - Se hace una copia de seguridad de la configuración anterior como *dir_instalación*/config/${hostname}_yn.xml.bak. Puede restaurar la configuración anterior si es necesario.
   - Puede pulsar Ctrl-C para salir del script cuando ejecute *dir_instalación*/*código_plataforma*/yn/bin/wxs-agent-config.sh config. La configuración existente no se cambia.

Configuración de la supervisión de WebSphere Extreme Scale en un entorno de WebSphere habilitado para la seguridad

Si instala WebSphere Extreme Scale en un entorno WebSphere Application Server con la seguridad habilitada, debe completar los pasos de configuración iniciales antes de configurar el Agente de WebSphere Applications.

Acerca de esta tarea

Si desea supervisar los servidores de WebSphere Extreme Scale en entornos WebSphere Application Server habilitados para la seguridad, es necesario configurar los valores de seguridad manualmente.

El procedimiento se aplica al caso siguiente:

- Los servidores de WebSphere Extreme Scale deben desplegarse dentro de los servidores de aplicaciones WebSphere Application Server (o de los procesos de agente de nodo o DMGR).
- El Agente de WebSphere Applications debe desplegarse en un nodo en el que se esté ejecutando un servicio de catálogo de zonas de WebSphere Extreme Scale. Configure la supervisión del agente de

WebSphere Extreme Scale bajo este nodo y establézcalo de modo que se conecte a esta instancia de servicio de catálogo.

- Debe utilizarse una instancia de agente para supervisar sólo una zona de WebSphere Extreme Scale.

Procedimiento

1. Si la versión de JDK de WebSphere Application Server es anterior a 1.7, debe volver a configurar el Agente de WebSphere Applications para que utilice el mismo JRE que WebSphere Application Server.
   a) Abra el archivo *dir_instalación*/config/.yn.environment.
   b) Añada el valor siguiente a la primera línea.

   ```
   #JAVAHOME=/opt/IBM/WebSphere/AppServer/java/8.0/jre
   ```

2. Configure el archivo de propiedades de seguridad del Agente de WebSphere Applications.

   Para obtener instrucciones, consulte "Configuración del agente para que funcione con archivos JAR y propiedades de seguridad de WebSphere Application Server" en la página 958.
3. Opcional: Si se utiliza un cliente Java™ seguro, debe asegurarse de que la autenticación se ha configurado correctamente. Debe editar el archivo de propiedades del cliente y el archivo de propiedades SSL. Para obtener instrucciones, consulte "Configuración de credenciales de conexión" en la página 959.

   Nota: Si la clave no está protegida por valores SSL, sólo debe especificar una contraseña y un nombre de usuario, y puede saltarse este paso.
4. Ejecute el script de configuración para iniciar la consola de configuración. Consulte "Ejecución de la configuración" en la página 961.

Configuración del agente para que funcione con archivos JAR y propiedades de seguridad de WebSphere Application Server

Configure el Agente de WebSphere Applications para que funcione con archivos JAR y propiedades de seguridad de WebSphere Application Server.

Acerca de esta tarea

Para realizar esta configuración, edite el archivo kynwb.properties.

Procedimiento

1. Abra el archivo *dir_instalación*/*código_plataforma*/yn/config/kynwb.properties. Si este archivo no existe, cree uno.
   - *dir_instalación* es el directorio de instalación del Agente de WebSphere Applications.
   - *código_plataforma* es el código de la plataforma en el que se instala el agente, por ejemplo, lx8266 representa Linux x86_64 R2.6 (64 bits), aix536 representa AIX R5.3 (64 bits).
2. Al principio del archivo, se indica la vía de acceso de clases. Añada las líneas siguientes antes de las líneas existentes.
   - Para WebSphere Application Server 9.0:

     ```
     inicio_servidor_aplicaciones/plugins/com.ibm.ws.runtime.jar:\
     inicio_servidor_aplicaciones/lib/bootstrap.jar:\
     inicio_servidor_aplicaciones/runtimes/com.ibm.ws.admin.client_9.0.jar:\
     inicio_servidor_aplicaciones/lib/wsogclient.jar:\
     ```

   - Para WebSphere Application Server 8.5:

     ```
     inicio_servidor_aplicaciones/plugins/com.ibm.ws.runtime.jar:\
     inicio_servidor_aplicaciones/lib/bootstrap.jar:\
     inicio_servidor_aplicaciones/runtimes/com.ibm.ws.admin.client_8.5.0.jar:\
     inicio_servidor_aplicaciones/lib/wsogclient.jar:\
     ```

   Ejemplo de una vía de acceso de clases modificada:

```
/opt/IBM/WebSphere/plugins/com.ibm.ws.runtime.jar:\
/opt/IBM/WebSphere/lib/bootstrap.jar:\
/opt/IBM/WebSphere/runtimes/com.ibm.ws.admin.client_8.5.0.jar:\
/opt/IBM/WebSphere/lib/wsogclient.jar:\
lib/kynwb.jar:\
lib/kynwxssec_api.jar:\
lib/itcam.cg.mbean.jar:\
wasdc/7.3/installer/lib/itcamfwas.jar:\
```

3. Al final del archivo *dir_instalación*/*código_plataforma*/yn/config/kynwb.properties, añada las líneas que indican los archivos de propiedades de seguridad que el agente debe utilizar. Normalmente, estos archivos son los que utiliza el programa de utilidad wsadmin:

```
-Dcom.ibm.CORBA.ConfigURL=file:/perfil_servidor_aplicaciones/properties/sas.client.props
-Dcom.ibm.SSL.ConfigURL=file:/perfil_servidor_aplicaciones/properties/ssl.client.props
```

   Si los valores de seguridad necesarios para el agente son distintos de los valores que utiliza el programa de utilidad wsadmin, cree copias independientes de los archivos y especifique vías de acceso a ellos, por ejemplo:

```
-Dcom.ibm.CORBA.ConfigURL=file:/opt/IBM/ITM/config/sas.client.props
-Dcom.ibm.SSL.ConfigURL=file:/opt/IBM/ITM/config/ssl.client.props
```

   Nota: Al instalar un fixpack o un arreglo temporal para el Agente de WebSphere Applications, los cambios que se realizan en los archivos yn.ini y kynwb.properties se sobrescriben. Por tanto, tras instalar un fixpack o arreglo temporal, debe volver a realizar los cambios en estos dos archivos.

Configuración de credenciales de conexión
Cuando se utiliza un cliente Java seguro, éste necesita leer un archivo de propiedades que contenga una lista de valores de CSIv2. Estos valores determinan cómo se autentica el cliente en un servidor. Debe asegurarse de que la autenticación está configurada adecuadamente.

Acerca de esta tarea

Normalmente, el archivo con estos valores se especifica en la propiedad de JVM com.ibm.CORBA.ConfigURL. Se pueden encontrar más valores de SSL en el archivo especificado en la propiedad de JVM com.ibm.SSL.ConfigURL.

Cuando el Agente de WebSphere Applications se configura para supervisar servidores de eXtreme Scale incorporados en WebSphere Application Server, actúa como cliente Java seguro. Por esta razón, -Dcom.ibm.CORBA.ConfigURL y -Dcom.ibm.SSL.ConfigURL se deben especificar en el archivo kynwb.properties.

En la mayoría de los casos, estas propiedades apuntan a los archivos sas.client.props y ssl.client.props del directorio *perfil_servidor_aplicaciones*/properties. Estos archivos los utilizan herramientas como wsadmin o xscmd. Por consiguiente, si puede utilizar una de estas herramientas para conectarse a un servidor de catálogo de Extreme Scale sin necesidad de especificar credenciales, no necesita personalizar los valores.

Si la conexión falla o necesita especificar un nombre de usuario o una contraseña, debe realizar una configuración adicional.

Modificación del archivo de propiedades de cliente
Edite el archivo sas.client.props que el Agente de WebSphere Applications debe utilizar.

Acerca de esta tarea
La vía de acceso completa al archivo sas.client.props se especifica en kynwb.properties, en la propiedad -Dcom.ibm.CORBA.ConfigURL. Especifique la información de conexión y seguridad para la instancia de WebSphere Application Server que ejecuta la instancia de Servicios de catálogo para la que está configurado el agente.

Procedimiento

1. Abra el archivo *perfil_servidor_aplicaciones*/properties/sas.client.props.
2. Cambie el valor de la propiedad com.ibm.CORBA.loginSource a properties:

   ```
   com.ibm.CORBA.loginSource=properties
   ```

3. Establezca la propiedad com.ibm.CORBA.securityServerHost en el nombre de host de un servidor de aplicaciones de la zona de WebSphere Extreme Scale. El servidor puede ser el servidor local o uno distinto. El servidor debe estar siempre disponible cuando se inicia el agente. Por ejemplo:

   ```
   com.ibm.CORBA.securityServerHost=server.company.com
   ```

4. Establezca la propiedad com.ibm.CORBA.securityServerPort en el puerto RMI para el perfil de servidor de aplicaciones, por ejemplo:

   ```
   com.ibm.CORBA.securityServerPort=2819
   ```

5. Establezca la propiedad com.ibm.CORBA.loginUserid en el nombre de inicio de sesión para comunicarse con el servidor de aplicaciones, y la propiedad com.ibm.CORBA.loginPassword en la contraseña, por ejemplo:

   ```
   com.ibm.CORBA.loginUserid=admin
   com.ibm.CORBA.loginPassword=password
   ```

6. Establezca las propiedades siguientes en true o false, de acuerdo con los valores de **Comunicaciones de entrada CSIv2** de la consola de administración de WebSphere:

   ```
   com.ibm.CSI.performTLClientAuthenticationRequired
   com.ibm.CSI.performTLClientAuthenticationSupported
   com.ibm.CSI.performTransportAssocSSLTLSRequired
   com.ibm.CSI.performTransportAssocSSLTLSSupported
   ```

   Las propiedades com.ibm.CSI.performTLClientAuthentication* están relacionadas con los valores de **Autenticación de certificados de cliente**. Las propiedades com.ibm.CSI.performTransportAssocSSLTLS* están relacionadas con los valores de **Transporte**.
7. Opcional: si no se utiliza el alias SSL predeterminado (DefaultSSLSettings), establezca el nombre de alias de configuración SSL en la propiedad com.ibm.ssl.alias.
8. Guarde el archivo y, a continuación, cifre la contraseña dentro del archivo sas.client.props. Para cifrar la contraseña, ejecute el mandato siguiente:

   - En sistemas Linux y UNIX, ejecute *perfil_servidor_aplicaciones*/bin/PropFilePasswordEncoder.sh sas.client.props com.ibm.CORBA.loginPassword

   Importante: Cuando la autenticación de certificado de cliente es necesaria y la autenticación básica está habilitada, es posible que también tenga que establecer la propiedad com.ibm.CORBA.validateBasicAuth=false.

Modificación del archivo de propiedades SSL de cliente
Modifique el archivo de propiedades SSL que el Agente de WebSphere Applications utiliza para acceder a certificados de servidor.

Acerca de esta tarea

Edite el archivo ssl.client.props que el agente debe utilizar. La vía de acceso completa al archivo se especifica en el archivo kynwb.properties, en la propiedad -Dcom.ibm.SSL.ConfigURL. Especifique la información de almacén de confianza y almacén de claves para la instancia de WebSphere Application Server que ejecuta la instancia de Servicios de catálogo para la que está configurado el agente.

Puede crear y gestionar certificados utilizando la consola de administración de WebSphere (**Seguridad** > **Gestión de claves y certificados SSL** > **Almacenes de claves y certificados**) o utilizando la herramienta iKeyman.

Procedimiento

1. Abra el archivo *perfil_servidor_aplicaciones*/properties/ssl.client.props.
2. Cambie el valor de la propiedad com.ibm.ssl.alias para que coincida con el valor de la misma propiedad en el archivo sas.client.props.

   Consejo: el archivo ssl.client.props puede contener varias configuraciones SSL. Cada configuración se inicia con la propiedad com.ibm.ssl.alias.
3. Establezca la propiedad com.ibm.ssl.enableSignerExchangePrompt en false.
4. Establezca las propiedades de almacén de claves siguientes para permitir que la aplicación cliente acceda a la clave de cifrado:

   com.ibm.ssl.keyStoreName
   El nombre que identifica este almacén de claves

   com.ibm.ssl.keyStore
   La vía de acceso completa y el nombre del archivo de almacén de claves

   com.ibm.ssl.keyStorePassword
   La contraseña del el almacén de claves

   com.ibm.ssl.keyStoreType
   Tipo de almacén de claves. Utilice el tipo PKCS12 predeterminado debido a su interoperatividad con otras aplicaciones.

   Importante: si la autenticación de certificado de cliente no es necesaria, el almacén de claves puede contener cualquier clave autofirmada. De lo contrario, el almacén de claves debe contener una clave que esté firmada por un certificado que esté en el almacén de confianza del servidor.
5. Establezca las siguientes propiedades de almacén de confianza para permitir que la aplicación cliente acceda a certificados de firmante:

   com.ibm.ssl.trustStoreName
   El nombre que identifica este almacén de confianza

   com.ibm.ssl.trustStore
   La vía de acceso completa y el nombre del archivo de almacén de confianza

   com.ibm.ssl.trustStorePassword
   La contraseña del almacén de confianza

   com.ibm.ssl.trustStoreType
   El tipo de almacén de confianza. Utilice el tipo PKCS12 predeterminado debido a su interoperatividad con otras aplicaciones.

   Importante: si el cliente va a utilizar una conexión SSL, el certificado de firmante del servidor debe estar en su almacén de confianza.

Ejecución de la configuración
Después de comprobar el entorno y la seguridad, puede ejecutar el proceso de configuración.

Procedimiento

1. Detenga el Agente de WebSphere Applications.
   a) Vaya al directorio *dir_instalación* donde se instala el Agente de WebSphere Applications.
   b) Ejecute el mandato bin/was-agent.sh stop.
2. Ejecute el script de configuración.

```
dir_instalación/código_plataforma/yn/bin/wxs-agent-config.sh config
```

Donde

- *dir_instalación* es el directorio de instalación de Agente de WebSphere Applications.
- *código_plataforma* es el código de la plataforma en el que se instala el agente, por ejemplo, lx8266 representa Linux x86_64 R2.6 (64 bits), aix536 representa AIX R5.3 (64 bits).

Mandato de ejemplo:

```
/opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh config
```

```
/opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh config
```

3. Cuando se le solicite la vía de acceso de instalación del agente, especifique el directorio de inicio del Agente de WebSphere Applications.

   Nota: El script busca el nombre del archivo de configuración en función de la vía de acceso de instalación que especifique. El valor predeterminado es *dir_instalación*/config/${hostname}_yn.xml. Si se le indica que el archivo no existe, podría deberse a que no se ha iniciado el Agente de WebSphere Applications antes de realizar esta configuración. Inicie el Agente de WebSphere Applications y deténgalo al menos una vez.
4. Cuando se le solicite el Tipo de conector del servidor de catálogo de WebSphere Extreme Scale, especifique 2 para continuar.
5. Cuando se le solicite Especificar un nombre de nodo para identificar este nodo de agente en la IU, especifique el nombre de nodo.

   El nombre de nodo se utiliza para identificar la zona de WebSphere Extreme Scale supervisada y se visualiza en el nombre de instancia que puede ver en la interfaz de usuario del Panel de instrumentos de Rendimiento de aplicaciones.
6. Cuando se le solicite ¿Seguridad de servidor de catálogo de WebSphere Extreme Scale habilitada?, especifique 1 para continuar. A continuación, especifique el nombre de usuario y la contraseña.
7. Especifique el nombre de host y el número de puerto del servidor de catálogo. Si hay varios servidores de catálogo, puede añadirlos de uno en uno. También puede añadir varias zonas una tras otra.

   - El nombre de host es el nombre del sistema donde está ubicado el servidor de catálogo. Asegúrese de que se puede acceder al nombre de host. De lo contrario, utilice la dirección IP como nombre de host.
   - El número de puerto indica el número **JMXServicePort** del servidor de catálogo de WebSphere Extreme Scale. Se hereda del valor de **BOOTSTRAP_ADDRESS** para cada WebSphere Application Server. Se pueden encontrar más detalles sobre el número de puerto en WebSphere Extreme Scale Knowledge Center.
8. Para iniciar el agente, ejecute el mandato siguiente.

   ```
   dir_instalación/bin/was-agent.sh start
   ```

   Nota:

   - La configuración del agente se almacena en *dir_instalación*/config/${hostname}_yn.xml. Si desea cambiar cualquier configuración, ejecute este script de nuevo o modifique el archivo .xml directamente.
   - Se hace una copia de seguridad de la configuración anterior como *dir_instalación*/config/${hostname}_yn.xml.bak. Puede restaurar la configuración anterior si es necesario.
   - Puede pulsar Ctrl-C para salir del script cuando ejecute *dir_instalación*/bin/wxs-agent-config.sh config. La configuración existente no se cambia.

Desconfiguración de la supervisión de WebSphere Extreme Scale
Cuando no desee supervisar WebSphere Extreme Scale, puede desconfigurar el Agente de WebSphere Applications.

Procedimiento

1. Detenga el Agente de WebSphere Applications.
   a) Vaya al directorio *dir_instalación* donde ha instalado el Agente de WebSphere Applications.
   b) Ejecute el mandato `bin/was-agent.sh stop`.
2. Ejecute el script de desconfiguración.

   ```
   dir_instalación/{pc}/yn/bin/wxs-agent-config.sh unconfig
   ```

   Donde

   - *dir_instalación* es el directorio de instalación del Agente de WebSphere Applications.
   - *código_plataforma* es el código de la plataforma en el que se instala el agente, por ejemplo, lx8266 representa Linux x86_64 R2.6 (64 bits), aix536 representa AIX R5.3 (64 bits).

   Mandato de ejemplo:

   ```
   /opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh unconfig
   ```

   ```
   /opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh unconfig
   ```

Configuración de la supervisión de WebSphere Infrastructure Manager

Configure el Agente de WebSphere Infrastructure Manager para supervisar el rendimiento de WebSphere Deployment Manager y el agente de nodo.

Acerca de esta tarea

El Agente de WebSphere Infrastructure Manager es un agente de múltiple instancia. Deberá crear la primera instancia e iniciar el agente manualmente.

Procedimiento

1. Para configurar el agente, ejecute el mandato siguiente.

   ```
   dir_instalación/bin/wim-agent.sh config
   nombre_instancia
   ```

   Donde *nombre_instancia* es el nombre que desea dar a la instancia y *dir_instalación* es el directorio de instalación del Agente de WebSphere Infrastructure Manager. El directorio de instalación predeterminado es `/opt/ibm/apm/agent`.
2. Cuando se le solicite `Editar valores de 'Monitoring Agent for WebSphere Infrastructure Manager'`, especifique `1` para continuar.
3. Cuando se le pida el valor para `Java home`, especifique el directorio donde está instalado Java.

   El valor predeterminado es `/opt/ibm/apm/agent/JRE/lx8266/jre`.
4. Cuando se le solicite el `Inicio de perfil DMGR`, especifique el directorio de inicio del perfil de Deployment Manager.

   El directorio predeterminado es `/opt/IBM/WebSphere/AppServer/profiles/Dmgr01`.
5. Cuando se le solicite el `ID de usuario de JMX`, especifique el ID de usuario utilizado para conectar con el servidor de MBean.
6. Cuando se le solicite `Especificar contraseña de JMX`, especifique la contraseña para el usuario.
7. Cuando se le solicite `Reescribir contraseña de JMX`, vuelva a especificar la contraseña.
8. Para iniciar el agente, ejecute el mandato siguiente.

   ```
   dir_instalación/bin/wim-agent.sh start nombre_instancia
   ```

Resultados
Ha creado una instancia de Agente de WebSphere Infrastructure Manager y ha iniciado el agente de supervisión para empezar a recoger muestras de datos para la supervisión de recursos.

Configuración de la supervisión de WebSphere MQ

Antes de iniciar el agente, debe asignar un nombre de instancia al agente y completar las diversas tareas de configuración para el ID de usuario y los nombres de sistema gestionado. Opcionalmente, también puede habilitar el rastreo de transacciones para el agente.

Antes de empezar

- Las instrucciones siguientes son para el release más reciente de este agente. Para obtener información sobre cómo comprobar la versión de un agente en el entorno, consulte Mandato de versión de agente. Para obtener información detallada sobre la lista de versiones de agente y de las novedades de cada versión, consulte "Historial de cambios" en la página 52.
- Asegúrese de que los requisitos del sistema del Agente de WebSphere MQ se cumplen en su entorno. Para obtener información actualizada sobre los requisitos del sistema, consulte el Informe de requisitos del sistema detallados para el Agente de WebSphere MQ.

Acerca de esta tarea

Las instrucciones son para el release más reciente del agente, a excepción de lo indicado.

Para configurar el entorno para el Agente de WebSphere MQ, antes debe asegurarse de el ID de usuario del agente pueda acceder a objetos de IBM MQ (WebSphere MQ), configurar IBM MQ (WebSphere MQ) para la habilitación de datos y, a continuación, configurar el Agente de WebSphere MQ.

El procedimiento siguiente es una hoja de ruta para configurar el Agente de WebSphere MQ, que incluye los pasos obligatorios y opcionales. Siga los pasos necesarios según sus necesidades.

Procedimiento

1. Autorice el ID de usuario utilizado para configurar, iniciar y detener el agente para acceder a los objetos de IBM MQ (WebSphere MQ). Consulte "Autorizar a los ID de usuario para ejecutar el agente" en la página 965.
2. Configure IBM MQ(WebSphere MQ) para habilitar los datos que desea supervisar. Consulte "Configuración de IBM MQ (WebSphere MQ) para la habilitación de datos" en la página 966.
3. Configure el agente, para ello, proporcione un nombre de instancia de agente, un nombre de gestor de colas y, de forma opcional, un nombre de agente. Consulte "Configuración del Agente de WebSphere MQ" en la página 968.
4. Opcional: Dependiendo de sus requisitos de supervisión, puede que necesite un nombre de sistema gestionado exclusivo para distinguir agentes de supervisión diferentes. Utilice la opción `Nombre de agente` en el mandato `mq-agent.sh config` para especificar el calificador medio del nombre de sistema gestionado. Consulte "Especificación de nombres de sistema gestionado exclusivos para varios gestores de colas" en la página 971.
5. Opcional: Para configurar el agente para recopilar los datos de rastreo de transacciones del gestor de colas supervisadas, utilice la página **Configuración de agente**. Para obtener instrucciones, consulte "Configuración del rastreo de transacciones para el Agente de WebSphere MQ" en la página 973.
6. Opcional: Habilite el agente para recopilar los datos históricos a largo plazo para colas y canales. Si desea más instrucciones, consulte "Habilitación de la recopilación de datos para el historial a largo plazo de colas y canales" en la página 974.
7. Opcional: Para supervisar remotamente el gestor de colas en MQ Appliance, es necesaria una configuración adicional en el agente y en IBM MQ (WebSphere MQ). Para obtener instrucciones, consulte las secciones "Supervisión remota de gestores de colas en MQ Appliance" en la página 976 o "Supervisión remota de los gestores de colas HA en MQ Appliance" en la página 977.

Autorizar a los ID de usuario para ejecutar el agente

Para que un ID de usuario pueda configurar, iniciar y detener el Agente de WebSphere MQ, el ID de usuario debe pertenecer al grupo **mqm**, que tiene privilegios administrativos completos sobre IBM MQ (WebSphere MQ). Además, para un usuario no root o un usuario no administrador, debe otorgar a los usuarios el acceso a los objetos de IBM MQ (WebSphere MQ) utilizando el mandato de control de IBM MQ (WebSphere MQ).

Acerca de esta tarea

En un sistema AIX o Linux, debe añadir el ID de usuario al grupo **mqm** y, a continuación, otorgar al ID de usuario el acceso adecuado a los objetos de IBM MQ (WebSphere MQ) con el mandato **setmqaut**.

En sistemas Windows, debe añadir el ID de usuario al grupo **mqm**. Si el ID de usuario no pertenece al grupo de usuarios de administrador, también debe utilizar el Editor del Registro para otorgar permisos al ID de usuario para iniciar o detener el agente.

Procedimiento

- Linux AIX

  En sistemas AIX o Linux, siga estos pasos:

  a) Inicie la sesión en el sistema AIX o Linux mediante el ID root.

  b) Añada el ID de usuario que se utiliza para ejecutar el agente al grupo **mqm**.

  c) (WebSphere MQ V7.5 o posterior): si el ID de usuario no es un usuario root en el sistema AIX o Linux, establezca el nivel adecuado de autoridad para que el ID de usuario pueda acceder a los objetos de IBM MQ (WebSphere MQ) ejecutando el mandato siguiente:

  ```
  setmqaut -m gestor_colas -t qmgr -p ID_usuario +inq +connect +dsp +setid
  ```

  Donde *gestor_colas* es el nombre del gestor de colas de WebSphere MQ V7.5 o posterior e *ID_usuario* es el ID de usuario no root o no administrador para ejecutar el agente.

- Windows

  En sistemas Windows, siga estos pasos:

  a) Inicie una sesión en el sistema Windows como administrador del sistema.

  b) Añada el ID de usuario que se utiliza para ejecutar el agente al grupo **mqm**.

  c) Si el ID de usuario que se utiliza para iniciar, ejecutar y detener el agente no es miembro del grupo de administradores, utilice el Editor del Registro para establecer los permisos para el ID de usuario para asegurarse de que se puede iniciar y detener el agente satisfactoriamente:

  a. Pulse **Inicio** > **Ejecutar** y escriba `regedit.exe` para abrir el Editor del registro.

  b. En el Editor del Registro, localice la clave `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`.

  c. Pulse con el botón derecho del ratón en la clave y pulse **Permisos**.

  d. Si el ID de usuario del Agente de WebSphere MQ no está en el Grupo o la lista de nombres de usuario, pulse **Añadir** para añadir el ID de usuario a la lista.

  e. Pulse el ID de usuario en la lista.

  f. En la lista Permisos para el *ID-usuario*, donde *ID_usuario* es el ID de usuario del Agente de WebSphere MQ, seleccione **Control total** en la columna Permitir y pulse **Aceptar**.

  g. En el Editor del Registro, localice la clave `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`.

  h. Pulse con el botón derecho del ratón en la clave y pulse **Permisos**.

  i. Si el ID de usuario del Agente de WebSphere MQ no está en el Grupo o la lista de nombres de usuario, pulse **Añadir** para añadir el ID de usuario a la lista.

  j. Pulse el ID de usuario en el Grupo o la lista de nombres de usuario.

k. En la lista Permisos para el *ID-usuario*, donde *ID_usuario* es el ID de usuario del Agente de WebSphere MQ, seleccione **Lectura** en la columna Permitir y pulse **Aceptar**.

l. Cierre el Editor de registro.

m. Localice el directorio *dir_instalación*, donde *dir_instalación* es el directorio de instalación de agente.

n. Pulse con el botón derecho del ratón en el directorio y pulse **Propiedades**.

o. En la pestaña Seguridad, si el ID de usuario del Agente de WebSphere MQ no está en el Grupo o la lista de nombres de usuario, pulse **Editar** y, a continuación, **Añadir** para añadir el ID de usuario a la lista.

p. Pulse el ID de usuario en el Grupo o la lista de nombres de usuario.

q. En la lista Permisos para el *ID_usuario*, en la columna Permitir, seleccione **Control completo**, donde **ID_usuario** es el ID de usuario del Agente de WebSphere MQ.

r. Pulse **Aceptar**.

Qué hacer a continuación

El próximo paso consiste en configurar IBM MQ (WebSphere MQ) para la habilitación de datos. Consulte "Configuración de IBM MQ (WebSphere MQ) para la habilitación de datos" en la página 966.

Configuración de IBM MQ (WebSphere MQ) para la habilitación de datos

Antes de configurar el Agente de WebSphere MQ, es aconsejable configurar IBM MQ (WebSphere MQ) para habilitar los datos que desea supervisar.

Acerca de esta tarea

Decida qué tipo de datos debe supervisar el Agente de WebSphere MQ. Habilite los datos en el gestor de colas mediante los mandatos de MQSC si el gestor de colas no genera los datos de forma predeterminada.

Recuerde: debe iniciar MQSC para el gestor de colas de destino antes de emitir los mandatos MQSC. Para obtener una lista del gestor de colas, emita el mandato **dspmq** desde el directorio `bin` del directorio de instalación de IBM MQ (WebSphere MQ). Para iniciar MQSC para un gestor de colas, emita el mandato siguiente desde el directorio `bin`, donde *<nombre_gestor_colas>* es el nombre del gestor de colas que desea configurar.

```
runmqsc <nombre_gestor_colas>
```

Procedimiento

- Para ver la antigüedad del mensaje de más antigüedad de una cola, realice los pasos que se indican en "Habilitación de la supervisión en tiempo real para las colas" en la página 966.
- Para supervisar determinados sucesos de gestor de colas no generados por el gestor de colas de forma predeterminada, siga los pasos indicados en la sección "Habilitación de la supervisión de sucesos para el gestor de colas" en la página 967.
- Para obtener los datos de rastreo de transacciones, siga los pasos indicados en la sección "Habilitación del rastreo de actividad de aplicación MQI" en la página 967.
- Para supervisar un gestor de colas remoto, asegúrese de que Agente de WebSphere MQ puede recopilar datos de supervisión mediante un canal en el sistema remoto. Para obtener más información, consulte "Valores de seguridad para la supervisión remota" en la página 968.

Habilitación de la supervisión en tiempo real para las colas

Acerca de esta tarea

Para ver la antigüedad del mensaje de más antigüedad (en segundos) en una cola, debe habilitar la supervisión en tiempo real para la cola.

Procedimiento

Utilice los mandatos siguientes para habilitar la supervisión en tiempo real para las colas en el entorno.

- Para habilitar la supervisión en tiempo real para todas las colas cuyo atributo MONQ está establecido en QMGR, emita el mandato siguiente:

  ```
  ALTER QMGR MONQ(nivel_recopilación)
  ```

  donde *nivel_recopilación* especifica el nivel de recopilación de los datos de supervisión para las colas. Puede establecerlo en LOW, MEDIUM o HIGH para ajustarlo a los requisitos de su entorno.
- Para habilitar la supervisión en tiempo real para la cola individual, emita el mandato siguiente:

  ```
  ALTER QLOCAL(nombre_cola) MONQ(nivel_recopilación)
  ```

  donde *nombre_cola* es el nombre de la cola; *nivel_recopilación* especifica el nivel de recopilación de los datos de supervisión para las colas. Puede establecerlo en LOW, MEDIUM o HIGH para ajustarlo a los requisitos de su entorno.

Resultados
Los datos se pueden visualizar en el widget de grupo Antigüedad de mensaje más antiguo para cola una vez que se haya iniciado Agente de WebSphere MQ.

Habilitación de la supervisión de sucesos para el gestor de colas

Acerca de esta tarea

La supervisión de sucesos es una de las técnicas de supervisión disponibles para supervisar la red de IBM MQ. Tras habilitar el gestor de colas para emitir determinados tipos de sucesos, los mensajes de suceso se colocan en colas de sucesos cuando se produce el suceso. De ese modo, el Agente de WebSphere MQ puede supervisar y visualizar estos mensajes de suceso.

Los siguientes tipos de sucesos no se supervisan ni se muestran con la configuración predeterminada del gestor de colas. Utilice el mandato **ALTER QMGR** para habilitar el gestor de colas para generar estos sucesos a fin de que puedan visualizarse en el Panel de instrumentos del rendimiento de aplicaciones.

- Sucesos de canal
- Sucesos de rendimiento

Procedimiento

Utilice los mandatos siguientes para habilitar el gestor de colas para generar los sucesos que desee supervisar:

- Para generar sucesos de canal, emita `ALTER QMGR CHLEV(ENABLED)`.
- Para generar sucesos de rendimiento, emita `ALTER QMGR PERFMEV(ENABLED)`.

Resultados
Los sucesos supervisados pueden visualizarse en el widget de grupo Sucesos del gestor de colas una vez iniciado el Agente de WebSphere MQ.

Habilitación del rastreo de actividad de aplicación MQI

Acerca de esta tarea
Para que los datos de rastreo de transacciones puedan visualizarse en los paneles de instrumentos de middleware y topología, debe habilitarse el rastreo de actividad de aplicación MQI en el gestor de colas.

Procedimiento

- Para habilitar la recopilación de información de rastreo de actividad de aplicación MQI, emita el siguiente mandato de MQSC:

```
ALTER QMGR ACTVTRC(ON)
```

Valores de seguridad para la supervisión remota

Acerca de esta tarea

Para utilizar Agente de WebSphere MQ para supervisar un gestor de colas remoto, debe asegurarse de que los valores de seguridad de IBM MQ (WebSphere MQ) no impiden que el agente recopile datos de supervisión mediante un canal en el sistema remoto.

El procedimiento siguiente proporciona un ejemplo de un valor de seguridad simple para la supervisión remota. Para ejercer un control más preciso sobre el acceso que se otorga a los sistemas que se conectan a nivel de canal, puede utilizar los registros de autenticación de canal. Para obtener más información, consulte Documentación de los mecanismos de seguridad de IBM MQ.

Procedimiento

1. Inhabilite la autenticación de canal mediante el siguiente mandato MQSC:

```
ALTER QMGR CHLAUTH(DISABLED) CONNAUTH(' ')
```

2. Cambie los valores de canal de la forma siguiente, donde *channel_for_remote_monitor* es el nombre del canal utilizado para la supervisión remota.
   - Linux AIX

```
ALTER CHANNEL(canal_para_supervisión_remota) CHLTYPE(SVRCONN) MCAUSER('mqm')
```

   - Windows

```
ALTER CHANNEL(canal_para_supervisión_remota) CHLTYPE(SVRCONN) MCAUSER(MUSR_MQADMIN)
```

3. Renueve los valores de seguridad.

```
REFRESH SECURITY
```

Configuración del Agente de WebSphere MQ

Debe asignar un nombre de instancia al Agente de WebSphere MQ y configurar el agente antes de poder empezar a supervisar el entorno de IBM MQ (WebSphere MQ).

Antes de empezar

- Asegúrese de que el ID de usuario del agente tenga el permiso adecuado para acceder a objetos de IBM MQ (WebSphere MQ). Si aún no lo ha hecho, siga las instrucciones de la sección “Autorizar a los ID de usuario para ejecutar el agente” en la página 965.
- Configure IBM MQ (WebSphere MQ) para habilitar la recopilación de datos necesaria. Si aún no lo ha hecho, consulte la sección “Configuración de IBM MQ (WebSphere MQ) para la habilitación de datos” en la página 966.
- Debe especificar el nombre del gestor de colas que el Agente de WebSphere MQ debe supervisar. Póngase en contacto con el administrador de IBM MQ (WebSphere MQ) si no conoce el nombre del gestor de colas adecuado. Como alternativa, emita el mandato **dspmq** desde el directorio `bin` del directorio de instalación de IBM MQ (WebSphere MQ) para obtener una lista de los gestores de colas. El valor QMNAME que se devuelve es el que debe suministrar al configurar el Agente de WebSphere MQ.

Acerca de esta tarea

El Agente de WebSphere MQ es un agente de varias instancias; debe crear la primera instancia e iniciar el agente de forma manual.

En sistemas UNIX o Linux, puede optar por configurar el agente con o sin interacciones. En sistemas Windows, sólo puede configurar el agente sin interacciones.

- Para configurar el agente con interacción, ejecute el script de configuración y responda a las solicitudes. consulte "Configuración interactiva" en la página 969.
- Para configurar el agente sin interacción, edite el archivo de respuestas silencioso y, a continuación, ejecute el script de configuración. Consulte "Configuración silenciosa" en la página 970.

Importante: Si también ha instalado Monitoring Agent for WebSphere MQ, que se entrega como un componente del producto de ITCAM for Applications, en el mismo sistema que el Agente de WebSphere MQ, que se entrega en Cloud APM, no los utilice para supervisar el mismo gestor de colas en el sistema.

Configuración interactiva

Procedimiento

Para configurar el agente mediante la ejecución del script y las respuestas a las solicitudes, siga estos pasos:

1. Especifique el mandato siguiente para crear una instancia de agente:

   ```
   dir_instalación/bin/mq-agent.sh config nombre_instancia
   ```

   donde *nombre_instancia* es el nombre que desea proporcionar a la instancia.
2. Cuando se le solicite el `Nombre del gestor de colas`, especifique el nombre del gestor de colas que se va a supervisar.
3. Cuando se le solicite el `Nombre de agente`, especifique el nombre de agente que se va a utilizar como el calificador medio del nombre del sistema gestionado. No pulse Intro para saltarse la especificación de este parámetro.

   Recuerde: Este nombre de agente es diferente del nombre de la instancia de agente. El nombre de instancia de agente se utiliza en el nombre del archivo de configuración de agente para distinguir los archivos de configuración entre agentes, por ejemplo, *nombre_host*_mq_*nombre_instancia*.cfg. El nombre de agente se utiliza como un identificador corto para crear nombres de sistema gestionado exclusivos. Para comprender cuándo es necesario un nombre de sistema gestionado exclusivo, consulte "Especificación de nombres de sistema gestionado exclusivos para varios gestores de colas" en la página 971.
4. Si desea supervisar un gestor de colas remoto, especifique los siguientes parámetros de configuración. Si desea supervisar un gestor de colas local, pulse Intro para continuar.

   - `Nombre de conexión`: El nombre de conexión para la supervisión remota. El formato es *dirección_IP* (*número_puerto*), por ejemplo, `127.0.0.1(1414)`. Si es la primera vez que configura la instancia de agente, puede pulsar Intro para aceptar el valor predeterminado de nulo. El nombre de conexión adecuada se puede descubrir automáticamente.
   - `Canal`: El nombre de canal utilizado para la recopilación remota de datos. Si es la primera vez que configura la instancia de agente, puede pulsar Intro para aceptar el valor predeterminado de nulo. Se utilizará el canal SYSTEM.DEF.SVRCONN.

   Limitación: No se pueden supervisar los registros de error de un gestor de colas remoto. Cuando el agente está supervisando un gestor de colas remoto, el panel de instrumentos Detalles de errores de MQ no contiene datos.
5. Cuando se le solicite la vía de acceso a biblioteca de WebSphere MQ, pulse Intro para aceptar el valor predeterminado, que es la vía de acceso a biblioteca de 64 bits de IBM MQ (WebSphere MQ) descubierta automáticamente por el Agente de WebSphere MQ. Si no se visualiza ningún valor predeterminado, debe proporcionar la vía de acceso a biblioteca de 64 bits de IBM MQ (WebSphere MQ) para continuar.
   Un ejemplo de vía de acceso de biblioteca de 64 bits es `/opt/mqm8/lib64` para un sistema Linux.
6. Para iniciar el agente, especifique el mandato siguiente:

   ```
   dir_instalación/bin/mq-agent.sh start nombre_instancia
   ```

Configuración silenciosa

Procedimiento

Para configurar el agente mediante la edición del archivo de respuestas silenciosas y la ejecución del script sin interacción, siga estos pasos:

1. Abra el archivo `mq_silent_config.txt` en un editor de texto.
   - Linux AIX *dir_instalación*`/samples/mq_silent_config.txt`
   - Windows *dir_instalación*`\tmaitm6_x64\samples\mq_silent_config.txt`

   donde *dir_instalación* es el directorio de instalación de Agente de WebSphere MQ.
2. Necesario: Para **QMNAME**, especifique el nombre del gestor de colas que se va a supervisar.
3. Necesario: Para **AGTNAME**, especifique el nombre de agente que se va a utilizar como el calificador medio del nombre del sistema gestionado.

   Recuerde: Este nombre de agente es diferente del nombre de la instancia de agente. El nombre de instancia de agente se utiliza en el nombre del archivo de configuración de agente para distinguir los archivos de configuración entre agentes, por ejemplo, *nombre_host*`_mq_`*nombre_instancia*`.cfg`. El nombre de agente se utiliza como un identificador corto para crear nombres de sistema gestionado exclusivos. Para comprender cuándo es necesario un nombre de sistema gestionado exclusivo, consulte "Especificación de nombres de sistema gestionado exclusivos para varios gestores de colas" en la página 971.
4. Si desea supervisar un gestor de colas remoto, especifique los siguientes parámetros de configuración:
   - **CONNAME**: El nombre de conexión para la supervisión remota. El formato es *dirección_IP*`(`*número_puerto*`)`, por ejemplo, `127.0.0.1(1414)`.
   - **CHANNEL**: El nombre de canal utilizado para la recopilación remota de datos. Si no se especifica, se utilizará el canal SYSTEM.DEF.SVRCONN.

   Limitación: No se pueden supervisar los registros de error de un gestor de colas remoto. Cuando el agente está supervisando un gestor de colas remoto, el panel de instrumentos Detalles de errores de MQ no contiene datos.
5. Opcional: Para **WMQLIBPATH**, especifique la vía de acceso de biblioteca de 64 bits de IBM MQ (WebSphere MQ). Por ejemplo, `/opt/mqm8/lib64`. Si no se especifica ningún valor, la vía de acceso se puede descubrir automáticamente durante la configuración del agente.
6. Guarde y cierre el archivo `mq_silent_config.txt` y, a continuación, ejecute el mandato siguiente desde la línea de mandatos:
   - Linux AIX *dir_instalación*`/bin/mq-agent.sh config` *nombre_instancia* *vía_acceso_archivo_respuestas*
   - Windows *dir_instalación*`\BIN\mq-agent.bat config` *nombre_instancia* `"`*vía_acceso_a_archivo_respuestas*`"`

   Donde *nombre_instancia* es el nombre de la instancia que configura, y *vía_acceso_archivo_respuestas* es la vía de acceso completa del archivo de respuestas silencioso.

   Recuerde: en sistemas Windows, no omita las comillas dobles ("") que incluyen la vía de acceso al archivo de respuestas silencioso, especialmente si la vía contiene caracteres especiales.

   Por ejemplo, si el archivo de respuestas está en el directorio predeterminado, ejecute el mandato siguiente.
   - Linux AIX

     ```
     /opt/ibm/apm/agent/bin/mq-agent.sh config nombre_instancia
     /opt/ibm/apm/agent/samples/mq_silent_config.txt
     ```
   - Windows

```
C:\IBM\APM\BIN\mq-agent.bat config nombre_instancia
"C:\IBM\APM\tmaitm6_x64\samples\mq_silent_config.txt"
```

7. Para iniciar el agente, especifique el mandato siguiente:
   - Linux AIX

     ```
     dir_instalación/bin/mq-agent.sh start nombre_instancia
     ```

   - Windows

     ```
     dir_instalación\bin\mq-agent.bat start nombre_instancia
     ```

Resultados

Ahora, puede iniciar la sesión en la Consola de Cloud APM y utilizar el editor de aplicaciones para añadir la instancia del Agente de WebSphere MQ al Panel de instrumentos del rendimiento de aplicaciones. Si desea instrucciones sobre cómo iniciar la Consola de Cloud APM, consulte "Inicio de la Consola de Cloud APM" en la página 1009. Para obtener información sobre cómo utilizar el editor de aplicaciones, consulte "Gestión de aplicaciones" en la página 1133.

Qué hacer a continuación

- Si ha habilitado la recopilación de información de rastreo de actividad de aplicación MQI en el gestor de colas, utilice la página **Configuración de agente** para configurar el Agente de WebSphere MQ para recopilar datos de rastreo de transacciones del gestor de colas supervisado. Consulte "Configuración del rastreo de transacciones para el Agente de WebSphere MQ" en la página 973. Si el agente no se muestra en la página **Configuración de agente** , reinicie el Servidor de Cloud APM.
- Dependiendo de sus requisitos de supervisión, puede que necesite un nombre de sistema gestionado exclusivo para distinguir agentes de supervisión diferentes. Utilice la opción `Nombre de agente` en el mandato `mq-agent.sh config` para especificar el calificador medio del nombre de sistema gestionado. Consulte "Especificación de nombres de sistema gestionado exclusivos para varios gestores de colas" en la página 971.
- Para configurar el Agente de WebSphere MQ para la supervisión remota, debe realizar algo de configuración manual después de crear una instancia de agente. Si desea instrucciones, consulte los temas siguientes:
  - "Supervisión remota de gestores de colas en MQ Appliance" en la página 976
  - "Supervisión remota de los gestores de colas HA en MQ Appliance" en la página 977

Especificación de nombres de sistema gestionado exclusivos para varios gestores de colas

A veces, son necesarios nombres de sistema gestionado exclusivos para distinguir agentes de supervisión diferentes que se conectan al mismo Servidor de Cloud APM. Utilice el parámetro **AGTNAME** en el archivo de respuestas silencioso o la opción `Nombre de agente` en el mandato **mq-agent.sh config** para especificar el calificador intermedio que se utiliza en el nombre del sistema gestionado.

Acerca de esta tarea

Cuando se inicia el Agente de WebSphere MQ, registra el siguiente sistema gestionado:

```
nombre_gestor_colas_supervisado:nombre_agente:MQ
```

donde

- *;nombre_gestor_colas_supervisado* es el nombre del gestor de colas que el agente está supervisando.
- *nombre_agente* es el calificador medio del nombre de sistema gestionado. Si no se especifica el valor *nombre_agente*, no se utiliza ningún valor.

La especificación del nombre de agente es útil en las circunstancias siguientes:

- Si su sitio tiene varios gestores de colas con el mismo nombre que se están ejecutando en distintos nodos, especifique el nombre de agente para cada gestor de colas, para que el Agente de WebSphere MQ pueda crear nombres exclusivos de sistema gestionado.
- Si la longitud del nombre de sistema gestionado supera los 32 caracteres, 2 nombres de gestor de colas diferentes pueden resolverse en el mismo nombre al quedar recortados. Para distinguir los nombres de sistemas gestionados para gestores de colas, especifique el nombre del agente para cada gestor de colas.
- Si desea agrupar e identificar los nombres de gestor de colas por algo que no sea el nombre de host y el nombre del gestor de colas, por ejemplo, un nombre de clúster de alta disponibilidad.
- Si desea permitir que varios agentes que están conectados al mismo Servidor de Cloud APM supervisen los gestores de colas con el mismo nombre en varios hosts.

Configuración interactiva

Procedimiento

Para utilizar la opción `Nombre de agente` en el mandato **`mq-agent.sh config`**, realice los siguientes pasos:

1. En la línea de mandatos, ejecute el mandato siguiente para empezar la configuración del Agente de WebSphere MQ.

   ```
   ./mq-agent.sh config nombre_instancia
   ```

   donde *nombre_instancia* es el nombre de la instancia que ha iniciado.
2. Siga las opciones para configurar la instancia de agente.

   Se necesita el nombre del gestor de colas. Para otras opciones, si no se necesita ningún cambio, utilice el valor predeterminado.
3. Cuando aparece la opción `Nombre de agente`, especifique el calificador medio para el nombre del sistema gestionado.

   Recuerde: El nombre completo del sistema gestionado es *nombre_gestor_colas_supervisado*:*nombre_agente*:MQ. La longitud máxima para el nombre completo del sistema gestionado es 32 caracteres, por lo que la longitud máxima para el calificador medio *nombre_agente* depende de la longitud del nombre del gestor de colas. Si el valor especificado para la opción `Nombre de agente` sobrepasa la longitud máxima, el valor de *nombre_agente* se trunca en no menos de 8 caracteres.

   Por ejemplo, para supervisar un gestor de colas llamado PERSONNEL en el nodo AIX1 mientras otro gestor de colas llamado PERSONNEL está en un nodo llamado LINUX2, ejecute primero el mandato siguiente para el nodo AIX1:

   ```
   ./mq-agent.sh config PERSONNEL
   ```

   Especifique el nombre del agente cuando aparece la opción *Nombre de agente*:

   ```
   Nombre de agente (el valor predeterminado es: ): AIX1
   ```

   Para supervisar simultáneamente el gestor de colas PERSONNEL en el nodo LINUX2, ejecute primero el mandato siguiente:

   ```
   ./mq-agent.sh config PERSONNEL
   ```

   A continuación, especifique el nombre de agente:

   ```
   Nombre de agente (el valor predeterminado es: ): LINUX2
   ```

Recuerde: Los nombres de los nodos de agente se utilizan para la opción `Nombre de agente` en los ejemplos de código solo a modo de explicación. Puede especificar otras series para la opción `Nombre de agente`.

Configuración silenciosa

Procedimiento

Para utilizar el parámetro **AGTNAME** en el archivo de respuestas silencioso, realice los siguientes pasos:

1. Abra el archivo de respuestas silencioso `mq_silent_config.txt` en un editor de texto.
2. Especifique un nombre de agente para el parámetro **AGTNAME**.

   Recuerde: El nombre completo del sistema gestionado es *nombre_gestor_colas_supervisado*:*nombre_agente*:MQ. La longitud máxima para el nombre completo del sistema gestionado es 32 caracteres, por lo que la longitud máxima para el calificador medio *nombre_agente* depende de la longitud del nombre del gestor de colas. Si el valor especificado para el parámetro **AGTNAME** sobrepasa la longitud máxima, el valor de *nombre_agente* se trunca en no menos de 8 caracteres.
3. Guarde y cierre el archivo `mq_silent_config.txt` y, a continuación, ejecute el mandato siguiente desde la línea de mandatos:

   ```
   dir_instalación/BIN/mq-agent.sh config nombre_instancia vía_acceso_de_archivo_respuestas
   ```

   Donde *nombre_instancia* es el nombre de la instancia que configura, y *vía_acceso_archivo_respuestas* es la vía de acceso completa del archivo de respuestas silencioso.

Qué hacer a continuación
Inicie la sesión en la Consola de Cloud APM. Si la instancia de agente con el MSN anterior se sigue visualizando como fuera de línea, edite la aplicación para eliminarlo y luego añada la nueva instancia de agente con el nombre de agente asignado.

Configuración del rastreo de transacciones para el Agente de WebSphere MQ

Los datos de rastreo de transacciones de IBM MQ (WebSphere MQ) se pueden visualizar en los paneles de instrumentos de middleware y topología tras habilitar la recopilación de datos en la página **Configuración de agente** del Agente de WebSphere MQ.

Antes de empezar

- Asegúrese de que la recopilación de información de rastreo de actividad de aplicación MQI esté habilitada en el gestor de colas. Si no lo ha hecho antes de configurar e iniciar el Agente de WebSphere MQ, siga las instrucciones de la sección "Habilitación del rastreo de actividad de aplicación MQI" en la página 967 y luego reinicie el agente.
- Asegúrese de que la versión de IBM MQ (WebSphere MQ) que está utilizando esté soportada por la función de rastreo de transacciones. Para obtener información actualizada sobre IBM MQ (WebSphere MQ), consulte la declaración de los requisitos previos en Detailed System Requirements Report for the Agente de WebSphere MQ.
- Asegúrese de que el Agente de WebSphere MQ esté configurado para supervisar el gestor de colas. Para obtener instrucciones, consulte "Configuración del Agente de WebSphere MQ" en la página 968.

Recuerde: Asegúrese de que ha actualizado el Agente de WebSphere MQ a la versión más reciente. Debe actualizar el agente, así como configurar y habilitar el rastreo de transacciones para ver datos en algunos de los widgets, como por ejemplo el widget de volumen de mensajes.

Procedimiento

Para configurar el rastreo de transacciones para el Agente de WebSphere MQ, realice estos pasos:

1. En la barra de navegación, pulse **Configuración del sistema** > **Configuración del agente**.

Se mostrará la página **Configuración del agente**.

2. Pulse el separador **WebSphere MQ**.
3. Seleccione los recuadros de selección de los gestores de colas que desea supervisar y lleve a cabo una de las acciones siguientes de la lista **Acciones**:
   - Para habilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Habilitado**. El estado de la columna **Rastreo de transacciones** se actualizará a Habilitado.

     Consejo: El seguimiento de colas de alias y colas remotas está habilitado de forma predeterminada. Para reducir el volumen de datos del que se va a realizar el seguimiento, puede inhabilitar el seguimiento de las colas de alias y remota pulsando **Establecer seguimiento de cola de alias** > **Inhabilitado** de la lista **Acciones**. Después de que se inhabilite el seguimiento de las colas de alias y remota, se eliminarán dichas colas de la vista Topología de transacción.
   - Para inhabilitar el rastreo de transacciones, pulse **Establecer rastreo de transacciones** > **Inhabilitado**. El estado de la columna **Rastreo de transacciones** se actualizará a Inhabilitado.

Resultados

Habrá configurado el Agente de WebSphere MQ para realizar el seguimiento de los gestores de colas seleccionados. Los datos de rastreo de transacciones se pueden visualizar en los paneles de instrumentos de middleware y topología. Si desea más información, consulte "Adición de aplicaciones middleware al Application Performance Dashboard" en la página 102.

Habilitación de la recopilación de datos para el historial a largo plazo de colas y canales

De forma predeterminada, el historial a largo plazo de colas y el historial a largo plazo de canales no se recopila y no se visualiza en ningún panel de instrumentos o widget de grupo predefinidos. Sin embargo, puede habilitar el agente para que recopile datos de historial a largo plazo y utilizar después la pestaña **Detalles de atributo** para consultar los datos recopilados.

Antes de empezar

Asegúrese de que el Agente de WebSphere MQ está instalado y configurado. Para obtener información, consulte "Configuración del Agente de WebSphere MQ" en la página 968.

Acerca de esta tarea

El historial a largo plazo del canal o el historial a largo plazo de la cola puede ser útil para detectar problemas dentro de canales o colas individuales.

Si es usted un usuario de Tivoli Data Warehouse, el agente también puede enviar los datos de historial a largo plazo a Tivoli Data Warehouse para su proceso.

Procedimiento

Siga estos pasos para habilitar el Agente de WebSphere MQ para recopilar datos de historial de largo plazo de colas y datos de historial de largo plazo de canales:

1. Abra el archivo de entorno de agente siguiente con un editor de texto. Si el archivo `mq.environment` no existe, créelo usted mismo.
   - Linux AIX *dir_instalación*`/config/mq.environment`
   - Windows *dir_instalación*`\Config\KMQENV_`*instancia*

   donde:
   - *dir_instalación* es el directorio de instalación del agente. El valor predeterminado es `/opt/ibm/apm` en sistemas Linux y AIX y `C:\IBM\APM` en sistemas Windows.
   - *instancia* es el nombre de instancia del agente.
2. Habilite la recopilación de datos estableciendo el valor **LH_COLLECTION** en ENABLED.

```
LH_COLLECTION=ENABLED
```

3. Opcional: Si es usted un usuario de Tivoli Data Warehouse y desea que el agente envíe los datos recopilados a Tivoli Data Warehouse, establezca el valor del parámetro **LH_PVTHISTORY** en ENABLED.

   ```
   LH_PVTHISTORY=ENABLED
   ```

   Recuerde: Habilite esta opción solo si necesita que los datos recopilados se envíen a Tivoli Data Warehouse.
4. Guarde el cambio y reinicie el agente.

Resultados

A continuación Agente de WebSphere MQ empieza a recopilar los datos de historial a largo plazo de colas y los datos de historial a largo plazo de canales. Si especificó LH_PVTHISTORY=ENABLED, los datos del historial a largo plazo recopilados también se envían a Tivoli Data Warehouse.

Qué hacer a continuación

Utilice la pestaña **Detalles de atributo** para ver los datos recopilados en el panel de instrumentos para la instancia de agente configurada. Seleccione **Channel_Long-Term_History** o **Queue_Long-Term_History** de la lista **Conjunto de datos**. Para obtener más información sobre la pestaña **Detalles de atributo**, consulte “Creación de una página de tablas o un gráfico personalizados” en la página 1127.

Habilitación de la supervisión de estadísticas de cola para el gestor de colas de IBM MQ

De forma predeterminada, las estadísticas de cola no se recopilan y no se visualizan en ningún panel de instrumentos o widget de grupo predefinido. Sin embargo, puede habilitar el agente para que recopile estadísticas del gestor de colas y luego ver los datos recopilados.

Antes de empezar

Asegúrese de que el Agente de WebSphere MQ está instalado y configurado. Para obtener información, consulte “Configuración del Agente de WebSphere MQ” en la página 968.

Procedimiento

Siga estos pasos para habilitar el Agente de WebSphere MQ para que recopile datos estadísticos:

1. Configure el gestor de colas para recopilar información de estadísticas de cola. Ejecute el siguiente mandato MQSC:

   ```
   ALTER QMGR STATQ(ON)
   ```
2. Establezca el intervalo durante el cual se recopilan los datos de contabilidad. Ejecute el mandato siguiente:

   ```
   ALTER QMGR STATINT(n)
   ```

   Donde **n** es el número de segundos durante el cual se recopilan los datos de contabilidad.
3. Habilite la recopilación de información de estadísticas para una cola específica. Ejecute el siguiente mandato MQSC:

   ```
   ALTER QLOCAL(nombre_cola) STATQ(QMGR)
   ```

   Donde **nombre_cola** es el nombre de la cola cuya información de estadísticas desea recopilar.

Qué hacer a continuación

Utilice uno de los métodos siguientes para ver los datos de supervisión de estadísticas de cola MQ:

- Ver los datos de supervisión desde la pestaña **Detalles de atributo** del conjunto de datos **MQ_Queue_Statistics**. Para obtener más información sobre la pestaña **Detalles de atributo**, consulte “Creación de una página de tablas o un gráfico personalizados” en la página 1127.

- Definir los umbrales basados en **Recuento de mensajes caducados** y otras métricas de **MQ_Queue_Statistics**. Para obtener más información sobre los umbrales, consulte "Umbrales y grupos de recursos" en la página 1010.

Supervisión remota de gestores de colas en MQ Appliance

Puede utilizar Agente de WebSphere MQ para supervisar el gestor de colas remoto en el entorno de MQ Appliance.

Antes de empezar

- Instale el Agente de WebSphere MQ en una plataforma soportada.
- Instale IBM MQ Client. La versión del cliente MQ debe ser la misma que la versión del gestor de colas MQ remoto.

Procedimiento

1. Configure la conexión con el gestor de colas remoto. En el gestor de colas remoto, defina un canal de conexión de servidor y un escucha que se utilice para la comunicación con el agente de supervisión. Ejecute el mandato siguiente:

```
M2000# mqcli
M2000(mqcli)#runmqsc gestor_colas_remoto
> DEFINE LISTENER(escucha) TRPTYPE(TCP)
PORT(número_puerto)
> DEFINE
CHANNEL(nombre_canal)CHLTYPE(SVRCONN)
TRPTYPE(TCP)
CONNAME('IP_host(número_puerto)')
QMNAME(gestor_colas_remoto)
> END
```

   donde:

   - *gestor_colas_remoto* es el nombre del gestor de colas remoto.
   - *escucha* es el nombre del escucha en el gestor de colas remoto.
   - *número_puerto* es el número de puerto que se va a utilizar para el escucha.
   - *nombre_canal* es el nombre que asigna a ambos canales, servidor y cliente.
   - *IP_host* es la dirección IP del sistema remoto.
2. Configure el escucha para iniciarse automáticamente y, después, inicie el escucha en el gestor de colas remoto ejecutando los mandatos siguientes en el sistema remoto:

```
M2000# mqcli
M2000(mqcli)#runmqsc gestor_colas_remoto
> ALTER LISTENER(escucha) TRPTYPE(tcp)
CONTROL(gestor_colas_remoto)
> START LISTENER(escucha)
> END
```

3. Asegúrese de que los valores de autenticación del canal están configurados de forma apropiada para el ID de usuario que se utiliza para iniciar la instancia de agente de MQ. Para obtener más información, consulte Configuración de un gestor de colas para aceptar conexiones de cliente en IBM MQ Appliance Knowledge Center.
4. Cree una instancia del Agente de WebSphere MQ para la supervisión remota siguiendo las instrucciones de "Configuración del Agente de WebSphere MQ" en la página 968 y proporcione información de conexión del gestor de colas remoto en las solicitudes que siguen a **Valores de supervisión remota**.

```
Valores de supervisión remota (Para un gestor de colas local, pulse Intro en
esta sección):
Nombre de conexión para la supervisión remota, por ejemplo: 192.168.1.1 (1415)
Nombre de conexión (el valor predeterminado es: null):
```

```
Nombre de canal para la supervisión remota, SYSTEM.DEF.SVRCONN es el valor predeterminado.
Canales (el valor predeterminado es: null):
```

5. Inicie la instancia del Agente de WebSphere MQ.

Supervisión remota de los gestores de colas HA en MQ Appliance

Para supervisar remotamente el gestor de colas HA en MQ Appliance, tiene dos opciones. Una es utilizar una sola instancia de agente para conectarse a cualquier sistema que tenga el gestor de colas activo. La otra opción es utilizar una instancia de agente separada para cada dispositivo en el cual se podría estar ejecutando el gestor de colas.

Acerca de esta tarea

Aquí solo se explica la segunda opción. Para utilizar distintas instancias de agente, necesita dos instalaciones de Agente de WebSphere MQ en sistemas Linux o UNIX. En sistemas Windows, solo necesita una instalación del agente y crear instancias de agente separadas.

Procedimiento

- Linux AIX

  Realice los pasos siguientes para utilizar el Agente de WebSphere MQ instalado en sistemas Linux o UNIX para la supervisión remota:

  a) Instale Agente de WebSphere MQ en distintos directorios en el sistema.

  b) Cree una instancia de cada Agente de WebSphere MQ instalado. Si desea más instrucciones, consulte “Configuración del Agente de WebSphere MQ” en la página 968.

  c) Modifique el archivo de configuración de cada instancia de agente para permitir la supervisión remota sustituyendo el contenido con las líneas siguientes:

  ```
  SET GROUP NAME (GROUP1) -
  DEFAULT(YES) -
  RETAINHIST(120) -
  COMMAND (YES) -
  MSGACCESS(DESC) -
  EVENTS(REMOVE) -
  ACCOUNTINGINFO(REMOVE) -
  STATISTICSINFO(REMOVE)

  SET MANAGER NAME(nombre_gestor_colas)
  REMOTE(YES)
  SET AGENT NAME(ID_agente)
  SET QUEUE NAME(*)
  MGRNAME(nombre_gestor_colas)
  QDEFTYPE(PREDEFINED)
  SET CHANNEL NAME(*)
  MGRNAME(nombre_gestor_colas)
  PERFORM STARTMON SAMPINT(300) HISTORY(NO)
  ```

  donde:

  – *nombre_gestor_colas* es el nombre del gestor de colas HA.

  – *ID_agente* es el ID para identificar el sistema del gestor de colas. Normalmente, el nombre de host o la dirección IP del sistema remoto donde se está ejecutando el gestor de colas HA.

  El nombre y la vía de acceso del archivo de configuración es *dir_instalación*/config/*nombre_host*_mq_*nombre_gestor_colas*.cfg.

  d) Cree un par de canales de cliente y servidor entre el gestor de colas primario y Agente de WebSphere MQ, entre el gestor de colas secundario y Agente de WebSphere MQ en el sistema remoto donde está instalado el gestor de colas primario.

  Recuerde: Debe ejecutar todos los mandatos siguientes antes de continuar hasta el siguiente paso.

  a. Ejecute los mandatos siguientes para el gestor de colas primario:

  ```
  M2000# mqcli
  M2000(mqcli)#runmqsc
  ```

```
gestor_colas_primario
>DEFINE LISTENER(escucha_primario)
TRPTYPE(TCP) PORT(número_puerto_primario)
>DEFINE
CHANNEL(nombre_canal_primario)
CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(nombre_canal_primario)
CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_host(número_puerto_primario)')
QMNAME(gestor_colas_primario)
```

donde:

- *gestor_colas_primario* es el nombre del gestor de colas primario.
- *escucha_primario* es el nombre del escucha para el gestor de colas primario.
- *número_puerto_primario* es el número de puerto utilizado por el escucha.
- *nombre_canal_primario* es el nombre que desea asignar a ambos canales, de servidor y cliente.
- *IP_host* es la dirección IP del sistema donde está instalado el gestor de colas primario.

b. Ejecute los mandatos siguientes para el gestor de colas secundario en el gestor de colas primario. Esto es para añadir la información de conexión del gestor de colas secundario al archivo de tabla de definición de canal de cliente del gestor de colas primario. A continuación, el mismo agente podrá conectarse automáticamente al gestor de colas secundario cuando el gestor de colas primario sufra una migración tras error.

```
>DEFINE
LISTENER(escucha_secundario)
TRPTYPE(TCP)
PORT(número_puerto_secundario)
>DEFINE
CHANNEL(nombre_canal_secundario)
CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE
CHANNEL(nombre_canal_secundario)
CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_host(número_puerto_secundario)')
QMNAME(gestor_colas_secundario)
```

donde:

- *gestor_colas_secundario* es el nombre del gestor de colas secundario en el sistema remoto. Este es el mismo que el nombre del gestor de colas primario.
- *escucha_secundario* es el nombre del escucha para el gestor de colas secundario.
- *número_puerto_secundario* es el número de puerto utilizado por el escucha.
- *nombre_canal_secundario* es el nombre que desea asignar a ambos canales, de servidor y cliente.
- *IP_host* es la dirección IP del sistema donde está instalado el gestor de colas secundario.

c. Por último, ejecute el mandato siguiente:

```
>END
>EXIT
```

e) Cree el archivo de tabla de definición de canal de cliente (AMQCLCHL.TAB) para la instancia del Agente de WebSphere MQ en el primer dispositivo MQ.

a. Utilice el mandato **runmqsc** o el mandato **runmqsc -n** para crear el archivo AMQCLCHL.TAB para el gestor de colas en el primer dispositivo MQ:

```
runmqsc -n
>DEFINE CHANNEL(nombre_canal_primario) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_host_dispositivo1(puerto_no_primario)') QMNAME(nombre_gestor_colas)
```

donde *IP_host_dispositivo1* es la dirección IP del primer dispositivo MQ; *nombre_canal_primario* y *puerto_no_primario* son los mismos que los definidos en el paso 4.

Consejo: de forma predeterminada, el archivo AMQCLCHL.TAB se crea en el directorio var/mqm/qmgrs/*nombre_gestor_colas*/@ipcc.

b. Mueva el archivo AMQCLCHL.TAB primario al directorio *dir_instalación_agente*/*arch*/mq/bin del sistema en el que está instalado el Agente de WebSphere MQ para el gestor de colas primario.

f) Cree el archivo de tabla de definición de canal de cliente (AMQCLCHL.TAB) para la instancia del Agente de WebSphere MQ en el segundo dispositivo MQ.

a. Utilice el mandato **runmqsc** o el mandato **runmqsc -n** para crear el archivo AMQCLCHL.TAB para el gestor de colas en el segundo dispositivo MQ:

```
runmqsc -n
>DEFINE CHANNEL(nombre_canal_secundario) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_host_dispositivo2(puerto_no_secundario)') QMNAME(nombre_gestor_colas)
```

donde *IP_host_dispositivo2* es la dirección IP del segundo dispositivo MQ; *nombre_canal_secundario* y *puerto_no_secundario* son los mismos que los definidos en el paso 4.

b. Mueva el archivo AMQCLCHL.TAB secundario al directorio *dir_instalación_agente*/*arch*/mq/bin del sistema en el que está instalado el Agente de WebSphere MQ para el gestor de colas secundario.

g) Asegúrese de que los valores de autenticación del canal están configurados de forma apropiada para el ID de usuario que se utiliza para configurar la conexión entre la instancia del agente y el gestor de colas.

h) Inicie todos los escuchas para ambos gestores de colas supervisados remotamente e inicie todas las instancias de Agente de WebSphere MQ.

- Windows

Realice los pasos siguientes para utilizar el Agente de WebSphere MQ instalado en sistemas Windows para la supervisión remota:

a) Instale el Agente de WebSphere MQ en el sistema Windows.

b) Cree dos instancias de Agente de WebSphere MQ para cada gestor de colas HA.

c) Modifique el archivo de configuración de cada instancia de agente para permitir la supervisión remota sustituyendo el contenido con las líneas siguientes:

```
SET GROUP NAME (GROUP1) -
DEFAULT(YES) -
RETAINHIST(120) -
COMMAND (YES) -
MSGACCESS(DESC) -
EVENTS(REMOVE) -
ACCOUNTINGINFO(REMOVE) -
STATISTICSINFO(REMOVE)

SET MANAGER NAME(nombre_gestor_colas)
REMOTE(YES)
SET AGENT NAME(ID_agente)
SET QUEUE NAME(*)
MGRNAME(nombre_gestor_colas)
QDEFTYPE(PREDEFINED)
SET CHANNEL NAME(*)
MGRNAME(nombre_gestor_colas)
PERFORM STARTMON SAMPINT(300) HISTORY(NO)
```

donde:

– *nombre_gestor_colas* es el nombre del gestor de colas HA.

– *ID_agente* es el ID para identificar el sistema del gestor de colas. Normalmente, el nombre de host o la dirección IP del sistema remoto donde se está ejecutando el gestor de colas HA.

Consejo: El nombre y la vía de acceso del archivo de configuración es *dir_instalación*\TMAITM6_x64\mq_<*nombre_instancia*>.cfg.

d) Cree un par de canales de cliente y servidor entre el gestor de colas primario y Agente de WebSphere MQ, entre el gestor de colas secundario y Agente de WebSphere MQ en el sistema remoto donde está instalado el gestor de colas primario.

Recuerde: Debe ejecutar todos los mandatos siguientes antes de continuar hasta el siguiente paso.

a. Ejecute los mandatos siguientes para el gestor de colas primario:

```
M2000# mqcli
M2000(mqcli)#runmqsc
gestor_colas_primario
>DEFINE LISTENER(escucha_primario)
TRPTYPE(TCP) PORT(número_puerto_primario)
>DEFINE
CHANNEL(nombre_canal_primario)
CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(nombre_canal_primario)
CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_host(número_puerto_primario)')
QMNAME(gestor_colas_primario)
```

donde:

- *gestor_colas_primario* es el nombre del gestor de colas primario.
- *escucha_primario* es el nombre del escucha para el gestor de colas primario.
- *número_puerto_primario* es el número de puerto utilizado por el escucha.
- *nombre_canal_primario* es el nombre que desea asignar a ambos canales, de servidor y cliente.
- *IP_host* es la dirección IP del sistema donde está instalado el gestor de colas primario.

b. Ejecute los mandatos siguientes para el gestor de colas secundario en el gestor de colas primario. Esto es para añadir la información de conexión del gestor de colas secundario al archivo de tabla de definición de canal de cliente del gestor de colas primario. A continuación, el mismo agente podrá conectarse automáticamente al gestor de colas secundario cuando el gestor de colas primario sufra una migración tras error.

```
>DEFINE
LISTENER(escucha_secundario)
TRPTYPE(TCP)
PORT(número_puerto_secundario)
>DEFINE
CHANNEL(nombre_canal_secundario)
CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE
CHANNEL(nombre_canal_secundario)
CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_host(número_puerto_secundario)')
QMNAME(gestor_colas_secundario)
```

donde:

- *gestor_colas_secundario* es el nombre del gestor de colas secundario en el sistema remoto. Este es el mismo que el nombre del gestor de colas primario.
- *escucha_secundario* es el nombre del escucha para el gestor de colas secundario.
- *número_puerto_secundario* es el número de puerto utilizado por el escucha.
- *nombre_canal_secundario* es el nombre que desea asignar a ambos canales, de servidor y cliente.
- *IP_host* es la dirección IP del sistema donde está instalado el gestor de colas secundario.

c. Por último, ejecute el mandato siguiente:

```
>END
>EXIT
```

e) Cree el archivo de tabla de definición de canal de cliente (`AMQCLCHL.TAB`) para cada instancia del Agente de WebSphere MQ.

a. Utilice el mandato **runmqsc** o el mandato **runmqsc -n** para crear el archivo AMQCLCHL.TAB para el gestor de colas en el primer dispositivo MQ:

```
runmqsc -n
>DEFINE CHANNEL(nombre_canal_primario) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_host_dispositivo1(puerto_no_primario)') QMNAME(nombre_gestor_colas)
```

donde *IP_host_dispositivo1* es la dirección IP del primer dispositivo MQ; *nombre_canal_primario* y *puerto_no_primario* son los mismos que los definidos en el paso 4.

b. Cree el archivo AMQCLCHL.TAB para el gestor de colas en el segundo dispositivo MQ:

```
runmqsc -n
>DEFINE CHANNEL(nombre_canal_secundario) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_host_dispositivo2(puerto_no_secundario)') QMNAME(nombre_gestor_colas)
```

donde *IP_host_dispositivo2* es la dirección IP del segundo dispositivo MQ; *nombre_canal_secundario* y *puerto_no_secundario* son los mismos que los definidos en el paso 4.

f) Renombre los dos archivos AMQCLCHL.TAB por nombres distintos, por ejemplo, NODE1.TAB y NODE2.TAB. Transfiéralos al directorio de *dir_instalación*\TMAITM6_x64, donde *dir_instalación* es el directorio de instalación de Agente de WebSphere MQ.

g) Modifique el archivo kmqcma_*nombre_instancia*.ini para establecer el valor **MQCHLTAB** en el archivo de la tabla de definición de canal de cliente para cada instancia de agente.
Por ejemplo, establezca MQCHLTAB=NODE1.TAB en el archivo kmqcma_instance1.ini y establezca MQCHLTAB=NODE2.TAB en el archivo kmqcma_instance2.ini.

h) Abra el editor de registros de Windows, localice la clave siguiente de **MQCHLTAB** y cámbiela de AMQCLCHL.TAB al archivo de tabla de definición de canal de cliente apropiado para cada instancia de agente.

- **HKEY_LOCAL_MACHINE\SOFTWARE\Candle\KMQ\Ver730*instancia1*\Environment**

  MQCHLTAB=*NODE1.TAB*

- **HKEY_LOCAL_MACHINE\SOFTWARE\Candle\KMQ\Ver730*instancia2*\Environment**

  MQCHLTAB=*NODE2.TAB*

i) Asegúrese de que los valores de autenticación de canal están configurados correctamente para el ID de usuario que se utiliza para configurar la conexión entre la instancia del agente y el gestor de colas.

j) Inicie todos los escuchas para ambos gestores de colas supervisados remotamente e inicie todas las instancias de Agente de WebSphere MQ.

Capítulo 8. Integración con otros productos y componentes

Puede integrar otros productos y componentes con IBM Cloud Application Performance Management para disponer de una sólida solución.

Integración con Cloud Event Management

Cloud Event Management proporciona gestión de incidencias en tiempo real entre los servicios, aplicaciones e infraestructura. Cuando se configura la integración entre Cloud Event Management e IBM Cloud Application Performance Management, todos los sucesos generados en Cloud APM se envían a Cloud Event Management.

Acerca de esta tarea

Configure un URL de webhook en Cloud Event Management. A continuación, configure Cloud APM para que utilice el URL de webhook para enviar sucesos a Cloud Event Management. Para obtener información adicional sobre Cloud Event Management, consulte el Knowledge Center de IBM Cloud Event Management.

Procedimiento

1. Pulse **Integraciones** en la página **Administración** de Cloud Event Management.
2. Pulse **Configurar una integración**.
3. Vaya al recuadro **IBM Cloud Application Performance Management** y pulse **Configurar**.
4. Escriba un nombre para la integración y pulse **Copiar** para añadir el URL de webhook generado al portapapeles. Asegúrese de guardar el webhook generado para que esté disponible más adelante en el proceso de configuración. Por ejemplo, puede guardarlo en un archivo.
5. Para empezar a recibir información de alertas desde Cloud APM, asegúrese de que **Habilitar gestión de sucesos de este origen** se ha establecido en `Activado` en Cloud Event Management.
6. Pulse **Guardar**.
7. Inicie la sesión en la suscripción Cloud APM.
8. Vaya a **Configuración del sistema** > **Configuración avanzada** > **Gestores de sucesos**. Para obtener más información, consulte Configuración avanzada.
9. Pegue el URL de webhook en el campo **Cloud Event Management Webhook**.
10. Pulse **Guardar**.

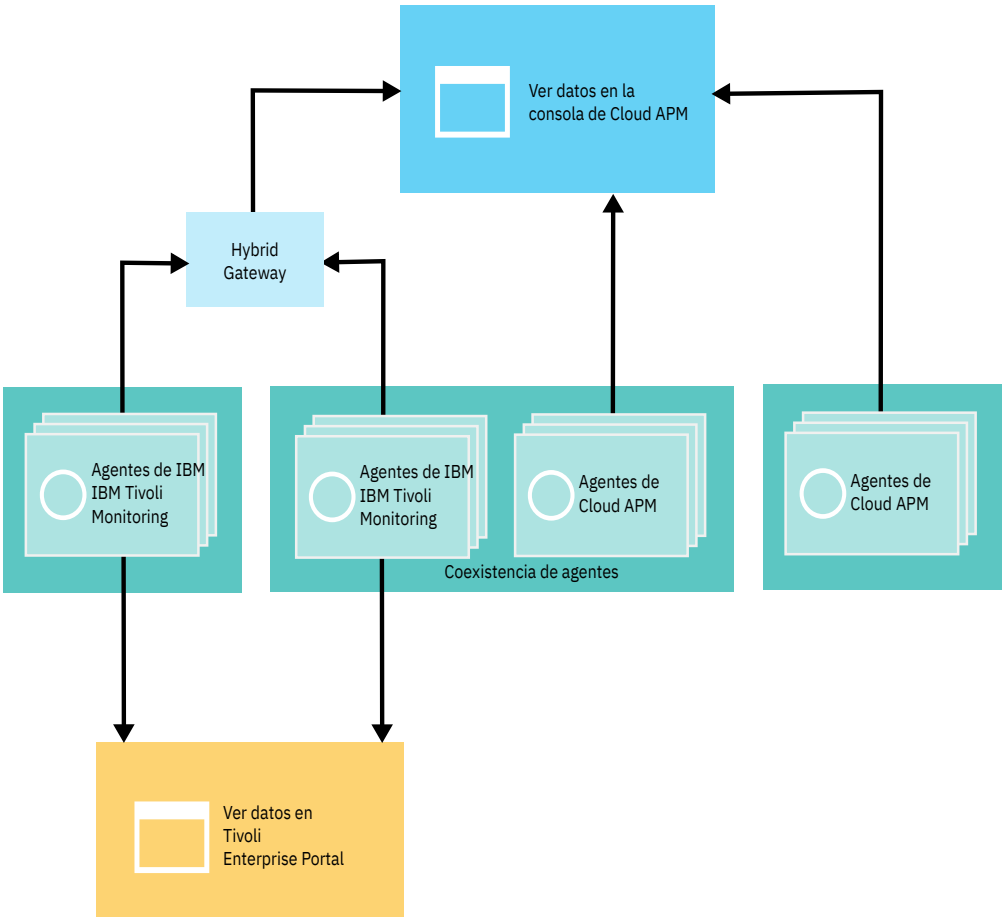
Integración con IBM Tivoli Monitoring V6.3

En un entorno que incluye los productos IBM Tivoli Monitoring e IBM Cloud Application Performance Management, puede utilizar estos productos juntos de varias maneras.

Las opciones siguientes están disponibles para integrarse con IBM Tivoli Monitoring:

- Puede instalar IBM Cloud Application Performance Management Hybrid Gateway para proporcionar una vista consolidada de los sistemas gestionados de uno o varios dominios de Tivoli Monitoring dominios y su dominio de Cloud APM en las páginas del Panel de instrumentos del rendimiento de aplicaciones. Si desea más información sobre la integración de agentes, consulte “Pasarela híbrida” en la página 987.
- Puede instalar agentes de Tivoli Monitoring y Cloud APM en el mismo sistema. Cuando coexisten agentes en el mismo sistema, pero no el mismo directorio, los datos de los agentes de Cloud APM están disponibles en la Consola de Cloud APM y los datos de los agentes de Tivoli Monitoring están

disponibles en Tivoli Enterprise Portal. Si los agentes que coexisten están supervisando los mismos recursos, se aplican ciertas limitaciones. Para obtener más información sobre la coexistencia de agentes, consulte “Coexistencia del agente de Cloud APM y el agente de Tivoli Monitoring” en la página 984.



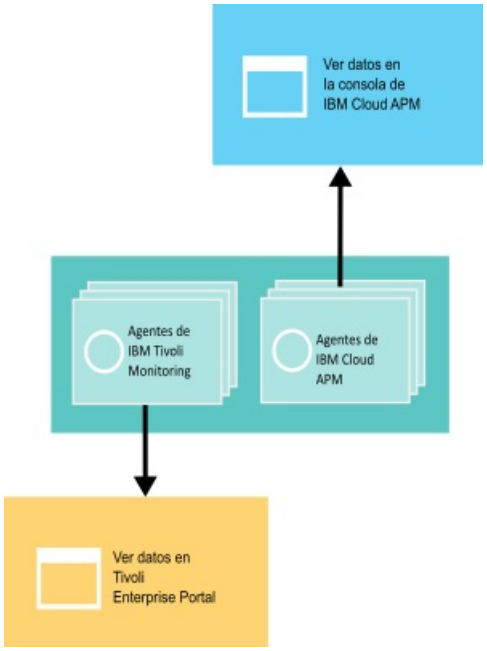
Coexistencia del agente de Cloud APM y el agente de Tivoli Monitoring

Se da soporte a la coexistencia de agentes. Puede instalar agentes de IBM Cloud Application Performance Management en el mismo sistema donde están instalados los agentes de IBM Tivoli Monitoring. Sin embargo, ambos tipos de agente no se pueden instalar en el mismo directorio.

Se hace referencia a los agentes de Cloud APM como agentes de versión 8. Se hace referencia a los agentes de Tivoli Monitoring como agentes de versión 6 o 7.

Cuando coexisten agentes en el mismo sistema, los datos de los agentes de versión 8 están disponibles en la Consola de Cloud APM y los datos de los agentes de versión 6 o 7 están disponibles en Tivoli Enterprise Portal.

Cuando los agentes de versión 6 o 7, que coexisten en el mismo sistema que los agentes de versión 8 y supervisan recursos distintos, están integrados con la IBM Cloud Application Performance Management Hybrid Gateway, los datos de ambos agentes están disponibles en la Consola de Cloud APM. Para obtener más información, consulte “Pasarela híbrida” en la página 987.



La tabla siguiente lista los agentes de Tivoli Monitoring con enlaces de documentación:

Tabla 236. Enlaces de documentación para agentes de Tivoli Monitoring

Agentes de Tivoli Monitoring	**Enlaces de documentación**
IBM Monitoring Agent for Citrix Virtual Desktop Infrastructure	IBM Tivoli Monitoring for Virtual Environments Knowledge Center
IBM Tivoli Monitoring for Virtual Environments Agent para Cisco UCS	Tivoli Monitoring for Virtual Environments Knowledge Center
IBM Tivoli Monitoring for Virtual Environments Agent for Linux Kernel-based Virtual Machines	Tivoli Monitoring for Virtual Environments Knowledge Center
IBM Tivoli Monitoring for Virtual Environments Agent for VMware VI	Tivoli Monitoring for Virtual Environments Knowledge Center
IBM Tivoli Monitoring: HMC Base Agent	IBM Tivoli Monitoring Knowledge Center
IBM Tivoli Monitoring: agente de sistema operativo Linux	Tivoli Monitoring Knowledge Center
IBM Tivoli Monitoring: agente de sistema operativo UNIX	Tivoli Monitoring Knowledge Center
IBM Tivoli Monitoring: agente de sistema operativo Windows	Tivoli Monitoring Knowledge Center
ITCAM Agent for DB2	ITCAM for Applications Knowledge Center
ITCAM Agent for HTTP Servers	ITCAM for Applications Knowledge Center
ITCAM Agent for J2EE	ITCAM for Applications Knowledge Center
ITCAM for Microsoft Applications: Microsoft Active Directory Agent	IBM Tivoli Composite Application Manager for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: agente de Microsoft Cluster Server	ITCAM for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: agente de Microsoft Exchange Server	ITCAM for Microsoft Applications Knowledge Center

Tabla 236. Enlaces de documentación para agentes de Tivoli Monitoring (continuación)	
Agentes de Tivoli Monitoring	**Enlaces de documentación**
ITCAM for Microsoft Applications: agente de Microsoft Hyper-V Server	ITCAM for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: agente de Microsoft Internet Information Services	ITCAM for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: agente de Skype for Business Server	ITCAM for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: agente de Microsoft .NET Framework	ITCAM for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: agente de Microsoft SharePoint Server	ITCAM for Microsoft Applications Knowledge Center
Monitoring Agent for Microsoft SQL Server	ITCAM for Microsoft Applications Knowledge Center
ITCAM Agent for SAP Applications	ITCAM for Applications Knowledge Center
ITCAM Agent for WebSphere Applications	IBM Tivoli Composite Application Manager for Application Diagnostics Knowledge Center para la versión 7.1 y anteriores y en ITCAM for Applications Knowledge Center para la versión 7.2 y posteriores.
ITCAM Agent for WebSphere DataPower Appliance	IBM Tivoli Composite Application Manager for Applications Knowledge Center
Monitoring Agent for WebSphere Message Broker	ITCAM for Applications Knowledge Center
Monitoring Agent for WebSphere MQ	ITCAM for Applications Knowledge Center
ITCAM Extended Agent for Oracle Database	ITCAM for Applications Knowledge Center
ITCAM Monitoring Agent para base de datos SAP HANA	Referencia de ITCAM Monitoring Agent para base de datos SAP HANA
ITCAM Web Response Time Agent	IBM Tivoli Composite Application Manager for Transactions Knowledge Center

Si los agentes que coexisten están supervisando los mismos recursos, el escenario siguiente no está soportado:

- Los agentes versión 6 o 7 están integrados con la Pasarela híbrida para visualizar datos de ambos agentes en la Consola de Cloud APM. Por ejemplo, si los agentes versión 6 o 7 están conectados al mismo Servidor de Cloud APM mediante la Pasarela híbrida, no utilice el Agente de IBM Integration Bus versión 8 y el Monitoring Agent for WebSphere Message Broker versión 6 o 7 para supervisar el mismo intermediario en su sistema.

Si un agente de Tivoli Monitoring, que está integrado con la Pasarela híbrida para visualizar datos en la Consola de Cloud APM, está supervisando un recurso y desea que el agente de Cloud APM supervise ese recurso, realice los pasos siguientes:

1. Elimine el agente de Tivoli Monitoring de las aplicaciones que lo incluyen.
2. Elimine el agente de Tivoli Monitoring del grupo de sistemas gestionados de Tivoli Monitoring que Cloud APM está configurado para utilizar.
3. Espere como mínimo 24 horas y, a continuación, instale el agente de Cloud APM, y añádalo a una aplicación.

Cuando agentes de varias instancias que coexisten en el mismo sistema, están integrados con la Pasarela híbrida, y supervisan los mismos recursos, utilice nombres diferentes para cada instancia para mostrar datos de ambos agentes en la Consola de Cloud APM.

Para los agentes con un recopilador de datos, se da soporte a dos agentes del mismo tipo. Se visualizan datos de diagnóstico detallado, recursos y rastreo de transacciones en la Consola de Cloud APM. Los datos de recursos se visualizan en Tivoli Enterprise Portal. Los agentes siguientes comparten un recopilador de datos:

Monitoring Agent for HTTP Server
El Agente de HTTP Server es un agente de Cloud APM y el ITCAM Agent for HTTP Servers es un agente de IBM Tivoli Monitoring. Si tiene ambos agentes en su entorno, puede configurar ambos recopiladores de datos en el mismo servidor HTTP para ambos agentes. Para obtener más información sobre la Agente de HTTP Server, consulte “Configuración de la supervisión de HTTP Server” en la página 278.

Agente de Microsoft .NET
Si desea más información sobre la coexistencia de Agente de Microsoft .NET, consulte “Habilitación del rastreo de transacciones en el entorno de coexistencia de agentes” en la página 547.

Agente de WebSphere Applications
Para obtener más información sobre la coexistencia de Agente de WebSphere Applications, consulte “Configuración del Agente de WebSphere Applications” en la página 891 y “Configuración del recopilador de datos para el entorno de coexistencia de agentes” en la página 892.

Pasarela híbrida

Para ver datos y sucesos de supervisión para los agentes de IBM Tivoli Monitoring y OMEGAMON en la Consola de Cloud APM, debe crear un grupo de sistemas gestionados e instalar la IBM Cloud Application Performance Management Hybrid Gateway en el dominio de Tivoli Monitoring, y configurar las comunicaciones en **Hybrid Gateway Manager** en la Consola de Cloud APM. Revise la información básica para ayudarle a planificar la instalación y configuración de una o variasPasarelas híbridas en los entornos de Tivoli Monitoring y Cloud APM.

Dónde instalar la Pasarela híbrida
Puede instalar la Pasarela híbrida en uno o varios dominios de Tivoli Monitoring: un hub Tivoli Enterprise Monitoring Server por dominio. Para obtener detalles sobre dónde instalar la Pasarela híbrida, consulte la información de Preparación de la instalación de la Pasarela híbrida. Para conocer los requisitos del sistema de la Pasarela híbrida, que incluyen Tivoli Enterprise Portal Server, consulte la pestaña **Prerequisites** del informe Hybrid Gateway Software Product Compatibility.

Agentes de Tivoli Monitoring y OMEGAMON soportados
Para que un agente de Tivoli Monitoring esté disponible para la Pasarela híbrida, también debe estar soportado en Cloud APM, con la excepción de los agentes de iOS y OMEGAMON. Para obtener una lista de versiones y agentes de Tivoli Monitoring disponibles, consulte Agentes soportados por la pasarela híbrida (APM Developer Center).

Para obtener una lista de los agentes de OMEGAMON que puede visualizar en la Consola de Cloud APM, consulte el tema Cómo empezar correspondiente a su release en el temario IBM OMEGAMON for Application Performance Management de IBM Knowledge Center.

Agentes de Tivoli Monitoring y OMEGAMON en la Consola de Cloud APM
Después de seleccionar la aplicación predefinida "Mis componentes" o una aplicación definida en el Panel de instrumentos del rendimiento de aplicaciones que incluye sistemas gestionados Tivoli Monitoring o OMEGAMON (o ambos), puede ver un panel de instrumentos de estado de resumen de todos los sistemas gestionados y un panel de instrumentos detallado de una sola instancia de sistema gestionado. También puede crear páginas de panel de instrumentos en la pestaña **Vistas personalizadas**.

Puede ver los sucesos de situación de estos agentes en la pestaña **Sucesos**. Sin embargo, no puede crear nuevos umbrales para los agentes de Tivoli Monitoring y OMEGAMON en el Gestor de umbrales. En su lugar, cree nuevas situaciones en Tivoli Monitoring.

no todos los sucesos de Tivoli Monitoring y OMEGAMON posibles están disponibles en el panel de instrumentos Sucesos. Solo se muestran los sucesos de nodos de agente que se pueden añadir a una aplicación. Por ejemplo, para el agente de Tivoli Monitoring para WebSphere Application Servers, se muestran los sucesos asociados a una instancia de servidor en particular, pero los sucesos del agente de forma global no se muestran.

Vea hasta 1500 sistemas gestionados del dominio de cada Tivoli Monitoring
El número máximo de sistemas gestionados, incluidos subnodos, que puede ver desde un dominio de Tivoli Monitoring es 1500. De forma predeterminada, el límite es 200 sistemas. Puede planificar dar soporte a una mayor cantidad de sistemas. Para obtener instrucciones, consulte "Planificación para un gran número de sistemas gestionados" en la página 996.

El límite para todos los dominios de Tivoli Monitoring debe estar dentro del máximo soportado por Cloud APM. Para obtener más información, consulte "Visión general de la arquitectura" en la página 45.

Solo supervisión de recursos
La supervisión de recursos está disponible para sus agentes de Tivoli Monitoring. Para obtener más información sobre la supervisión de recursos, consulte "Ofertas y complementos" en la página 47 y "Capacidades" en la página 54. Si tiene la suscripción de IBM Cloud Application Performance Management, Advanced, los paneles de instrumentos de rastreo de transacciones y diagnósticos no están disponibles para sistemas gestionados desde el entorno de Tivoli Monitoring.

Tivoli afecta a la disponibilidad de sistemas gestionados de Tivoli Monitoring
Para entornos de Tivoli Monitoring que incluyen Tivoli, los sistemas gestionados que están disponibles a través de la Pasarela híbrida se ven afectados por las políticas de autorización. Para obtener más información, consulte Utilización de políticas de autorización basadas en roles en el Tivoli Monitoring Knowledge Center.

Para ver una demostración en vídeo, consulte Integrating with Tivoli Monitoring - Pasarela híbrida.

Preparación de la instalación de la Pasarela híbrida

Para instalar la IBM Cloud Application Performance Management Hybrid Gateway, primero debe asegurarse de que su entorno está configurado correctamente. Revise la información para ayudarle a planificar la instalación de Pasarela híbrida.

Dónde instalar la Pasarela híbrida

La Pasarela híbrida debe instalarse en un sistema x86-64 Red Hat Enterprise Linux v6.2 (o posterior) que tenga una conexión de red con IBM Tivoli Monitoring e IBM Cloud Application Performance Management.

La Pasarela híbrida se puede instalar en el mismo sistema que Tivoli Enterprise Portal Server o en un sistema separado de Tivoli Enterprise Portal Server si los sistemas se ejecutan en Red Hat Enterprise Linux. Sin embargo, Pasarela híbrida no se puede instalar en el mismo sistema que el Servidor de Cloud APM.

Un dominio de Tivoli Monitoring tiene un hub Tivoli Enterprise Monitoring Server. Cuando el entorno de Tivoli Monitoring consta de varios dominios, puede instalar la Pasarela híbrida en más de un dominio.

Para conocer los requisitos de sistema relacionados con la Pasarela híbrida, pulse la pestaña **Hardware** de Pasarela híbrida Software Product Compatibility Report.

Configuración de Tivoli Enterprise Portal Server para la Pasarela híbrida

Para entornos de Tivoli Monitoring en los que el servidor de portal tenga una gran carga, debe instalar un servidor de portal dedicado aparte para dar servicio a las solicitudes de la Pasarela híbrida. Si configura un servidor de portal aparte:

- Puede utilizar el mismo host para el servidor de portal y la Pasarela híbrida si el servidor de portal está ejecutando Red Hat Enterprise Linux.
- Asegúrese de que el servidor de portal independiente tiene el soporte de aplicaciones para los agentes cuyos datos se visualizan en la Consola de Cloud APM.

- Asegúrese de que los clientes de Tivoli Enterprise Portal no están conectados al servidor de portal independiente para realizar tareas administrativas tales como crear espacios de trabajo personalizados, crear situaciones, y crear grupos de sistemas gestionados.

Tivoli Enterprise Portal Server debe ser V6.3 Fix Pack 6 o posterior. Si el servidor de portal tiene una versión anterior, los agentes de Tivoli Monitoring integrados quizá no estén disponibles para añadirlos a una aplicación en la Consola de Cloud APM.

El Proveedor de datos del panel de instrumentos de IBM Tivoli Monitoring debe estar habilitado en Tivoli Enterprise Portal Server. Para conocer los detalles, consulte Verificación de que dashboard data provider está habilitado en el conjunto de temas de IBM Tivoli Monitoring, en el IBM Knowledge Center.

Los puertos TCP que deben estar abiertos en la Pasarela híbrida
Los siguientes puertos TCP deben estar abiertos en Pasarela híbrida. Para cada puerto, uno de los lados envía una solicitud, y el otro proporciona una respuesta. Se indica el lado que inicia la conexión.

- Pasarela híbrida inicia una conexión unidireccional con el Servidor de Cloud APM en el puerto 443 y envía solicitudes HTTP.

  Si Pasarela híbrida utiliza un proxy de reenvío de paso a través para conectarse al Servidor de Cloud APM, configure Pasarela híbrida para que utilice el puerto de proxy en lugar del puerto 443 para las conexiones unidireccionales que inicia con el Servidor de Cloud APM. Para obtener instrucciones, consulte "Utilización de un proxy directo para comunicarse con el Servidor de Cloud APM" en la página 991.
- Si utiliza HTTP para comunicarse con el servidor de portal, abra el puerto 15200. Si utiliza HTTPS, abra el puerto 15201. La Pasarela híbrida inicia una conexión unidireccional con el servidor de portal en el puerto 15200 o 15201. Para utilizar un puerto personalizado, actualice el valor de **Puerto de Portal Server**. Para obtener más información, consulte "Gestor de Pasarela híbrida" en la página 997.

  De forma alternativa, si la Pasarela híbrida utiliza un proxy de reenvío de paso a través para conectar con el servidor de portal, configure la Pasarela híbrida para que el lugar de esto utilice el puerto de proxy para conexiones unidireccionales que inicie con el servidor de portal. Establezca el valor de **Puerto de proxy de paso a través**. Para obtener más información, consulte "Gestor de Pasarela híbrida" en la página 997.
- Para que Pasarela híbrida escuche sucesos EIF de entrada de Tivoli Enterprise Monitoring Server, abra el puerto 9998. El servidor de supervisión inicia una conexión unidireccional con la Pasarela híbrida en el puerto 9998. El programa de utilidad de instalación muestra un aviso si este puerto no está abierto.

Privilegios de root necesarios para ejecutar el script de instalación de la Pasarela híbrida
Debe ejecutar el script de instalación de la Pasarela híbrida con privilegios raíz. Para obtener una lista completa de sistemas operativos, consulte System requirements (APM Developer Center)

Instalación de la Pasarela híbrida
Descargue e instale la IBM Cloud Application Performance Management Hybrid Gateway para ver sistemas gestionados del dominio IBM Tivoli Monitoring en la Consola de Cloud APM.

Antes de empezar
Revise y complete las tareas de preparación necesarias de la sección Preparación de la instalación de la Pasarela híbrida.

Procedimiento

Siga estos pasos para instalar la Pasarela híbrida en su dominio de Tivoli Monitoring:

1. Descargue el paquete de Pasarela híbrida.

   El archivo `APM_Hybrid_Gateway_Install.tar` contiene la Pasarela híbrida y el script de instalación.

   a) Inicie la sesión con su cuenta y vaya a Productos y servicios en IBM Marketplace.

   b) En **IBM Cloud APM** pulse **Más acciones**.

c) Pulse **Mostrar paquetes adicionales**.

d) Seleccione **Hybrid Gateway**. Si es necesario, desplácese para encontrar la entrada.

e) Pulse **Descargar**.

2. Si es necesario, transfiera el archivo al sistema en el que se ejecutará la Pasarela híbrida.
3. Especifique el mandato siguiente para extraer los archivos:

```
tar -xf APM_Hybrid_Gateway_Install.tar
```

El archivo de archivado contiene un script que se utiliza para desplegar la Pasarela híbrida. El script de instalación se extrae en el directorio y los archivos de Pasarela híbrida se extraen en subdirectorios.

4. Vaya al directorio de Pasarela híbrida y ejecute el script de instalación con privilegios de usuario root:

```
cd APM_Hybrid_Gateway_Install_versión
./install.sh
```

donde *versión* es la versión actual, por ejemplo 8.1.4.0.

Se inicia una exploración de requisitos previos de su entorno y tarda varios minutos en completarse. Si faltan algunos requisitos, un mensaje le dirigirá a un archivo de registro que contiene la causa del error. Un requisito previo, como insuficiente espacio de disco, detendrá la instalación. Debe identificar el error y volver a iniciar la instalación. También puede desactivar la comprobación de requisitos previos tal como se describe en Omisión del escáner de requisitos previos.

5. Una vez que el sistema pasa la exploración de requisito previo, responda a la solicitud para aceptar el acuerdo de licencia seleccionando 1 para Sí.

Un mensaje le insta a iniciar la sesión en la Consola de Cloud APM y a configurar la Pasarela híbrida antes de continuar. También se visualiza el nombre de perfil predeterminado que se deriva del nombre de host.

6. Pulse Intro para aceptar el nombre predeterminado o especifique un nombre de perfil.

Si ya ha creado un perfil para este dominio de Tivoli Monitoring, utilice el mismo nombre que ha proporcionado en el Gestor de Pasarela híbrida. Si todavía no ha creado un perfil, puede aceptar el nombre predeterminado o proporcionar un nombre nuevo, pero asegúrese de apuntarse el nombre porque deberá utilizarlo más tarde al crear el perfil. (Consulte “Configurar la Pasarela híbrida utilizando la Consola de Cloud APM” en la página 993).

Después de pulsar Intro, la instalación de la Pasarela híbrida continúa.

Resultados

La Pasarela híbrida se instala en el directorio `/opt/ibm/hybridgateway` y se inicia automáticamente. El archivo de registro de instalación está en `/opt/ibm/hybridgateway/logs/install-hybridgateway-`*`timestamp`*`.log`. Los archivos de registro de Pasarela híbrida están en el directorio `/opt/ibm/wlp/usr/servers/hybridgateway/logs`. Tenga en cuenta que hasta que no se haya configurado la conexión con Tivoli Enterprise Portal Server, se registran los errores de conexión.

Qué hacer a continuación

- Puede configurar la Pasarela híbrida para utilizar un proxy directo para comunicar con el Servidor de Cloud APM. Si desea más instrucciones, consulte “Utilización de un proxy directo para comunicarse con el Servidor de Cloud APM” en la página 991.
- Puede comprobar el estado de la Pasarela híbrida con el mandato siguiente: *`dir_instalación`*`/hybridgateway/bin/hybridgateway.sh status`. Para otras opciones, consulte “Gestión de la Pasarela híbrida” en la página 997.
- Si no ha creado el grupo de sistemas gestionados para la Pasarela híbrida, siga las instrucciones en “Creación del grupo de sistemas gestionados” en la página 991.
- Si todavía no ha creado un perfil de Pasarela híbrida para el dominio de Tivoli Monitoring, siga las instrucciones de la “Configurar la Pasarela híbrida utilizando la Consola de Cloud APM” en la página 993.

- Si el entorno de Tivoli Monitoring tiene más de un dominio de hub, puede instalar la Pasarela híbrida en otros dominios. Repita los pasos de este procedimiento para instalar la Pasarela híbrida en otro dominio de Tivoli Monitoring.

Utilización de un proxy directo para comunicarse con el Servidor de Cloud APM
Puede configurar la IBM Cloud Application Performance Management Hybrid Gateway para utilizar un proxy directo para comunicar con el Servidor de Cloud APM.

Procedimiento

1. En el host donde ha instalado la Pasarela híbrida, edite el archivo `/opt/ibm/wlp/usr/servers/hybridgateway/bootstrap.properties`:
   - Si la Pasarela híbrida utiliza HTTP para comunicarse con el Servidor de Cloud APM, añada las líneas:

     ```
     http.proxyHost=host_proxy
     http.proxyPort=puerto_proxy
     ```

   - Si la Pasarela híbrida utiliza HTTPS para comunicarse con el Servidor de Cloud APM, añada las líneas:

     ```
     https.proxyHost=host_proxy
     https.proxyPort=puerto_proxy
     ```

   donde *host_proxy* es el nombre de host o la dirección IP del proxy, accesible desde el host de la Pasarela híbrida y *puerto_proxy* es el puerto del proxy.
2. Reinicie el Pasarela híbrida.

Creación del grupo de sistemas gestionados
Utilice el editor de grupo de objetos en el cliente de Tivoli Enterprise Portal para crear un grupo de los sistemas gestionados que desea ver en la Consola de Cloud APM.

Antes de empezar

- Los tipos de agentes de IBM Tivoli Monitoring y OMEGAMON que puede incluir en el grupo de sistemas gestionados deben estar entre los agentes soportados. Por ejemplo, para Tivoli Monitoring, algunos de los agentes soportados son Monitoring Agent for Oracle Database o Monitoring Agent for Linux OS.

  Para obtener la lista actual de agentes de Tivoli Monitoring soportados, consulte Agentes soportados por la pasarela híbrida (APM Developer Center). Para obtener una lista de los agentes de OMEGAMON que puede visualizar en la Consola de Cloud APM, consulte el tema Cómo empezar en el temario IBM OMEGAMON for Application Performance Management de IBM Knowledge Center.
- Los agentes de Tivoli Monitoring y OMEGAMON se deben conectar a la misma infraestructura de IBM Tivoli Monitoring. Si su entorno tiene varios dominios de Tivoli Monitoring, cree un grupo de sistemas gestionados para cada hub Tivoli Enterprise Monitoring Server para el que se instala una Pasarela híbrida.
- De forma predeterminada, puede añadir hasta 200 sistemas gestionados al grupo de sistemas gestionados para ver del dominio Tivoli Monitoring en el Panel de instrumentos del rendimiento de aplicaciones. Puede aumentar el límite hasta un máximo de 1500 sistemas siguiendo varios pasos de planificación. Para obtener más información, consulte “Planificación para un gran número de sistemas gestionados” en la página 996. Si tiene varias Pasarelas híbridas para Tivoli Monitoring en un entorno con varios hubs, el grupo de sistemas gestionados de cada dominio debe estar dentro del máximo soportado por Cloud APM. Para obtener más información, consulte Visión general de la arquitectura.
- El valor predeterminado para manejar subnodos ha cambiado en el release de Cloud APM marzo de 2017. En releases anteriores, si había agentes con subnodos, como por ejemplo el Agente de WebSphere Applications, era necesario asignar el nodo de gestión al grupo de sistemas gestionados, y todos los subnodos se incluían automáticamente. Aunque se asignaba un nodo de gestión al grupo de sistemas gestionados, los subnodos se incluían en el recuento del máximo de sistema gestionado.

En el release de Cloud APM marzo de 2017 y posteriores, los subnodos cuyos datos de métrica desea visualizar en la Consola de Cloud APM se deben asignar específicamente al grupo de sistemas gestionados.El agente de gestión se descubre automáticamente su alguno de sus subnodos se asigna claramente al grupo de sistemas gestionados. Para aplicaciones de supervisión basadas en subnodos, es posible que Cloud APM necesite consultar el agente de gestión para obtener la información necesaria para identificar claramente los recursos de supervisión que aparecen en el navegador del panel de instrumentos de Cloud APM. Es por esta razón que, con la versión actual de la modalidad de descubrimiento, el agente de gestión se incluye automáticamente y como mínimo un subnodo asociado se asigna al grupo de sistemas gestionado configurado para que lo utilice la Pasarela híbrida. La modalidad de descubrimiento actual da soporte al control preciso sobre los recursos de subnodo que pueden visualizarse en la Consola de Cloud APM y se alinea mejor con el modo de construcción de las aplicaciones de Cloud APM, particularmente de las aplicaciones que implican grandes conjuntos de instancias de recursos de subnodo. utilice siempre la modalidad de descubrimiento predeterminada actual al integrar agentes de OMEGAMON con Cloud APM.

Puede especificar la versión de modalidad de descubrimiento que la Pasarela híbrida utilizará asignando el valor adecuado a una propiedad externa denominada `MSN_DISCOVERY_MODE`, que Pasarela híbrida procesa durante la inicialización.Para controlar qué modalidad de descubrimiento utiliza la Pasarela híbrida, añada la propiedad `MSN_DISCOVERY_MODE` (o cambie su valor actual) al archivo de propiedades siguiente del sistema donde está instalada la Pasarela híbrida y, a continuación, reinicie la Pasarela híbrida.

```
dir_instalación_HG/wlp/usr/servers/hybridgateway/bootstrap.properties
```

Los valores posibles de la propiedad `MSN_DISCOVERY_MODE` son:

- `MSN_DISCOVERY_MODE=1` obliga a la Pasarela híbrida a utilizar la modalidad de descubrimiento de agente original, en la que todos los subnodos se descubren automáticamente para los agentes de gestión que se asignan al grupo de sistemas gestionados de Tivoli Monitoring.
- `MSN_DISCOVERY_MODE=2` obliga a la Pasarela híbrida a utilizar la nueva modalidad de descubrimiento de agente predeterminada, en la que la Pasarela híbrida sólo consulta los subnodos que están asignados claramente al grupo de sistemas gestionados . El agente o agentes de gestión asociados se descubren automáticamente.

- Si prefiere crear el grupo de sistemas gestionados con los mandatos **`tacmd createsystemlist`** y **`tacmd editsystemlist`** IBM Tivoli Monitoring, consulte *IBM Tivoli Monitoring: Consulta de mandatos* (https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) para obtener información sobre cómo ejecutar los mandatos.

Procedimiento

Siga estos pasos para crear un grupo de sistemas gestionados en el cliente de Tivoli Enterprise Portal.

1. Inicie el cliente de Tivoli Enterprise Portal con un ID de usuario y una contraseña que tenga acceso completo a todos los tipos de sistemas gestionados (**Aplicaciones permitidas** se establece en **Todas las aplicaciones** para el ID de usuario.)
2. Pulse en **Editor de grupos de objetos**.
3. Expanda el objeto **Sistema gestionado** y seleccione **Todos los sistemas gestionados** para combinar varios tipos de agentes (por ejemplo, sistema operativo Windows y Oracle) en el grupo de sistemas gestionados. Si prefiere que el grupo de sistemas gestionados solo contenga un tipo de agente de supervisión como, por ejemplo, Linux OS o aplicaciones WebSphere, seleccione el tipo de agente.
4. Pulse **Crear nuevo grupo** y especifique un nombre para el grupo de sistemas gestionados.

   El nombre puede constar de letras y números, y no puede tener ningún espacio, carácter de puntuación o caracteres especiales distintos al subrayado (_).

   Después de pulsar **Aceptar**, el nuevo grupo de sistemas gestionados se visualiza en la carpeta de sistemas gestionados.

5. Seleccione los sistemas gestionados de la lista **Sistemas gestionados disponibles** y para moverlos a la lista **Asignados**.

   Para seleccionar varios sistemas gestionados, mantenga pulsada la tecla Control mientras pulsa en cada sistema gestionado. Después de seleccionar un sistema gestionado, puede utilizar Mayús +pulsación para seleccionar todos los sistemas gestionados entre esta selección y la primera selección.
6. Después de añadir sistemas gestionados al grupo, pulse **Aceptar** para guardar los cambios y cerrar el editor de grupos de objetos.

Qué hacer a continuación

- Después de crear el grupo de sistemas gestionados e instalar Pasarela híbrida, debe configurar la Pasarela híbrida en la Consola de Cloud APM.
- Para la configuración, especifique el nombre del grupo de sistemas gestionados que ha creado, el ID de usuario de Tivoli Enterprise Portal que tiene permiso de acceso a todos los tipos de agente y el nombre de host y el puerto de Tivoli Enterprise Portal Server.
- Para obtener instrucciones de instalación, consulte "Instalación de la Pasarela híbrida" en la página 989.
- Para ver instrucciones de configuración, consulte "Configurar la Pasarela híbrida utilizando la Consola de Cloud APM" en la página 993.

Configurar la Pasarela híbrida utilizando la Consola de Cloud APM

Utilice la página **Hybrid Gateway Manager** en la Consola de Cloud APM para configurar la IBM Cloud Application Performance Management Hybrid Gateway para conectar con Tivoli Enterprise Portal Server y especificar el grupo de sistemas gestionados.Puede crear un perfil de Pasarela híbrida para cada Tivoli Enterprise Monitoring Server concentrador del entorno.

Procedimiento

Siga estos pasos para configurar la Pasarela híbrida en la Consola de Cloud APM.

1. Si no ha iniciado sesión en la Consola de Cloud APM, hágalo ahora.

   (Consulte "Inicio de la Consola de Cloud APM" en la página 1009).
2. Pulse **Configuración del sistema** > **Pasarela híbrida Manager**.

   La página se muestra con una tabla de cualquiera de las Pasarelas híbridas configuradas para sus dominios de Tivoli Monitoring. Si se visualiza un perfil con un nombre en blanco, corresponde a la Pasarela híbrida instalada antes del release agosto de 2017. Para obtener más información, consulte "Nombre de perfil" en la página 998.
3. Pulse **Añadir** para abrir la ventana **Añadir Pasarela híbrida**, especifique un nombre nuevo en el campo **Nombre de perfil** y pulse **Añadir**.

   Si ya ha instalado la Pasarela híbrida en el dominio de Tivoli Monitoring, asegúrese de utilizar el nombre proporcionado o aceptado durante la instalación de la Pasarela híbrida. El nombre de perfil especificado durante la instalación y el nombre que especifique aquí deben coincidir exactamente.

   Se abre la ventana **Editar pasarela híbrida**.
4. En el campo **Nombre de grupo de sistemas gestionados**, especifique el nombre del grupo de sistemas gestionados para la Pasarela híbrida.

   Este es el nombre que ha utilizado en "Creación del grupo de sistemas gestionados" en la página 991.
5. Especifique la dirección, el puerto y el protocolo de comunicación web de Tivoli Enterprise Portal Server:

Opción	Descripción
Nombre de host de Portal Server	Escriba la dirección IP del host del servidor de portal o el nombre de host totalmente calificado o nombre de dominio.

Opción	Descripción
Puerto de Portal Server	Especifique el número de puerto que utiliza el servidor de portal para las comunicaciones web. El puerto predeterminado es 15200 para HTTP o 15201 para HTTPS. El valor de 0 establece el puerto en el valor predeterminado 15200 para HTTP o 15201 para HTTPS.
Protocolo de Portal Server	Seleccione el protocolo internet **HTTP** o el protocolo internet **HTTPS** seguro para conectarse al servidor de portal.

6. Complete los campos **Nombre de usuario de Portal Server** y **Contraseña de Portal Server** con el nombre de usuario de inicio de sesión y la contraseña correspondiente para iniciar el cliente de Tivoli Enterprise Portal.

   El ID de usuario debe tener acceso a todos los tipos de agente de supervisión (**Aplicaciones permitidas** se establece en **Todas las aplicaciones**), por ejemplo, el ID `sysadmin`. Si desea más información, consulte Administrar usuarios en el Tivoli Monitoring IBM Knowledge Center.
7. Si el acceso al servidor de portal pasa a través de un servidor proxy, especifique la dirección, el puerto y el protocolo web:

Opción	Descripción
Nombre de host de proxy de paso a través	Especifique la dirección IP o el nombre completo del sistema host de proxy.
Puerto de proxy de paso a través	Especifique el número de puerto del sistema host de proxy.
Protocolo de proxy de paso a través	Seleccione el protocolo que se utiliza para las comunicaciones a través del proxy: HTTP o HTTPS

Resultados

Después de pulsar **Guardar**, se establece una conexión con el servicio de Pasarela híbrida y se descubren los sistemas gestionados del dominio de Tivoli Monitoring. El grupo de sistemas gestionados se sondea cada 5 minutos para datos de supervisión de recursos.

Qué hacer a continuación

- Debe configurar Tivoli Monitoring para que interactúe con Cloud APM. Para obtener instrucciones, consulte "Configuración de Tivoli Monitoring para la integración con Cloud APM" en la página 994.
- Puede repetir estos pasos para añadir un perfil para cada dominio de Tivoli Monitoring del que desea supervisar sistemas gestionados de Cloud APM.
- Puede gestionar perfiles existentes con las herramientas de **Hybrid Gateway Manager**:

  Seleccione una Pasarela híbrida y pulse **Editar** para abrir la ventana **Editar pasarela híbrida**.

  Seleccione una Pasarela híbrida que ya no desee y pulse **Suprimir**. Después de confirmar que desea suprimir la Pasarela híbrida, el perfil se eliminará permanentemente.

  Pulse una cabecera de columna para ordenar la tabla según esa columna; Control + clic en otra columna para añadir una clasificación secundaria.

  Pulse dentro del recuadro de texto de filtro y escriba el principio del valor por el que va filtrar. A medida que escribe, las filas que no coincidan con los criterios se filtrarán. Para borrar el filtro, pulse en el cuadro de filtro o pulse la tecla de retroceso.

Configuración de Tivoli Monitoring para la integración con Cloud APM

Para integrar el dominio de IBM Tivoli Monitoring con Cloud APM, debe realizar tareas como configurar Tivoli Enterprise Portal Server y configurar el hub Tivoli Enterprise Monitoring Server.

Procedimiento

Para cada dominio de Tivoli Monitoring en el que tenga instalado una Pasarela híbrida, siga estos pasos:

1. Configure el Tivoli Enterprise Portal Server para habilitar el proveedor de datos de panel de instrumentos.

   El proveedor de datos es necesario para integrar Cloud APM con la Pasarela híbrida. Si desea instrucciones, consulte los temas siguientes:

   - Windows Windows: Instalación del servidor de portal (paso 16c).
   - Linux AIX Configuración del servidor de portal en Linux o AIX: procedimiento de línea de mandatos (paso 14).

   Si utiliza la característica de espera activa, debe especificar una alteración temporal de dominio. La Pasarela híbrida utiliza el nombre de dominio para recopilar datos de ambos servidores de supervisión de hub, independientemente del hub al que está conectado el servidor de portal.
2. Si desea ver sucesos de situación de los agentes de Tivoli Monitoring en la Consola de Cloud APM, configure el servidor de supervisión de hub para uno de los casos siguientes:

   - Para enviar sucesos solo a la Pasarela híbrida.
   - Para enviar sucesos a la Pasarela híbrida y a receptores de EIF adicionales como por ejemplo servidores de Netcool/OMNIbus.

   Siga uno de estos pasos en función del caso aplicable.

   a) Para configurar el hub Tivoli Enterprise Monitoring Server para enviar sucesos solo a la Pasarela híbrida, siga los pasos del tema Configuración del servidor de supervisión concentrador para reenviar sucesos.

      Especifique el número de puerto 9998 para el parámetro **`ServerPort`**.
      Cloud APM no reenvía los sucesos de Tivoli Monitoring a Netcool/OMNIbus. Si desea ver los sucesos de Tivoli Monitoring en Cloud APM y en Netcool/OMNIbus, debe configurar Tivoli Monitoring para enviar los sucesos a los dos sistemas.

   b) Para configurar el hub Tivoli Enterprise Monitoring Server para enviar sucesos a la Pasarela híbrida y a otro receptor de EIF como por ejemplo un servidor de Netcool/OMNIbus, configure el receptor de EIF predeterminado siguiendo los pasos del tema Configuración del servidor de supervisión concentrador para reenviar sucesos.

      El tema proporciona también información sobre la creación de destinos de EIF adicionales mediante el mandato **`tacmd createEventDest`**. Especifique el puerto 9998 como el número de puerto de EIF para el destino de la Pasarela híbrida.

   c) Configure las situaciones que existan para los agentes en el grupo de sistemas gestionados de la Pasarela híbrida para asegurarse de que los sucesos de situación se envían al destino de EIF para la Pasarela híbrida. Para obtener instrucciones, consulte el tema Especificar qué situaciones reenvían sucesos a Netcool/OMNIbus.

Qué hacer a continuación

Revise Panel de instrumentos del rendimiento de aplicaciones para confirmar que los sistemas gestionados de su dominio de Tivoli Monitoring pasan a través de Pasarela híbrida:

1. Pulse **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** para abrir el panel de instrumentos **Todas mis aplicaciones**.
2. En el cuadro de resumen para "Mis componentes", pulse **Componentes** para abrir el panel de instrumentos de resumen para todos los sistemas gestionados por componentes (excepto Agente de WebSphere Applications). Si no tiene una aplicación "Mis componentes", añada una aplicación tal como se describe en “Gestión de aplicaciones” en la página 1133.
3. Busque sistemas gestionados de su dominio de Tivoli Monitoring, indicado por un icono de dominio de **ITM** (IBM Tivoli Monitoring) en el título de widget de grupo de resumen de estado. Si falta algún sistemas gestionado, vaya al Foro de Cloud Application Performance Management y busque "Pasarela híbrida".

Puede crear aplicaciones con sistemas gestionados desde los dominios de Tivoli Monitoring e incluir sistemas gestionados desde el dominio de Cloud APM. Para obtener más información, consulte "Gestión de aplicaciones" en la página 1133.

Planificación para un gran número de sistemas gestionados
El número máximo de sistemas gestionados que puede ver desde el dominio de IBM Tivoli Monitoring es 1500. Si incluye un agente que tiene subnodos en el grupo de sistemas gestionados creado para el perfil de la Pasarela híbrida, todos los subnodos, así como el agente, cuentan para el límite. De forma predeterminada, este límite es de 200 sistemas gestionados, pero puede realizar varios pasos de planificación para ampliar el límite.El límite para todos los dominios de Tivoli Monitoring debe estar dentro del máximo soportado por Cloud APM. Para obtener más información, consulte "Visión general de la arquitectura" en la página 45.

- Establezca el valor de variable de entorno de Tivoli Enterprise Portal Server **KFW_REPORT_NODE_LIMIT** en un número mayor o igual que el número de sistemas gestionados para la Pasarela híbrida. El valor predeterminado es 200. Para obtener instrucciones, consulte Valores de configuración de Tivoli Enterprise Portal Server.
  Si los sistemas gestionados sobrepasan este valor, el registro de mensajes de Tivoli Enterprise Portal Server `KfwServices` muestra un mensaje similar a este ejemplo:
  `56C6246F.0000-10:ctreportmanager.cpp,2864,"CTReport::Manager::executeDefinitionDual") La consulta se dirige a 1497 nodos que sobrepasa el límite actual de 200 nodos.`
- Si observa un gran número de sistemas, el rendimiento puede degradarse, dependiendo del tipo de agentes, la latencia de red entre la Pasarela híbrida y los sistemas gestionados, y el tamaño del entorno supervisado por cada agente (cantidad de datos recopilados y enviados). Para evitar este efecto, seleccione solo los agentes que proporcionan datos necesarios y asegure una conectividad de red veloz entre los sistemas gestionados y el host de la Pasarela híbrida.
- Al aumentar la latencia de red, también aumenta el tiempo de recopilación de datos de un número dado de agentes. la Pasarela híbrida intenta recopilar datos de cada agente cada 5 minutos. Si el tiempo para recopilar datos de todos los agentes sobrepasa los 5 minutos, la Pasarela híbrida pierde ejemplos de datos y, por tanto, las métricas no están disponibles en las páginas del Panel de instrumentos del rendimiento de aplicaciones.
- Para compensar velocidades de red muy bajas, puede intentar aumentar el número de hebras utilizadas por la Pasarela híbrida para recopilar ejemplos de datos. El parámetro **MAX_COLLECTOR_THREADS** del archivo `bootstrap.properties` de la Pasarela híbrida controla el número de hebras. El valor predeterminado es 50.

Desinstalación de la Pasarela híbrida
Si ya no desea ver los sistemas gestionados de IBM Tivoli Monitoring en la Consola de Cloud APM, desinstale la IBM Cloud Application Performance Management Hybrid Gateway.

Procedimiento

1. En el directorio Pasarela híbrida *dir_instalación*`/hybridgateway/bin` (como `/opt/ibm/hybridgateway/bin`), ejecute el mandato siguiente:

   ```
   ./hybridgateway.sh uninstall
   ```

   La Pasarela híbrida se elimina y un mensaje confirma que se ha desinstalado satisfactoriamente. Si tiene alguna aplicación en la Consola de Cloud APM que incluye agentes híbrido, los agentes híbridos siguen apareciendo hasta que la infraestructura de supervisión procesa su eliminación.
2. En la Consola de Cloud APM, pulse **Configuración del sistema** > **Pasarela híbrida Manager**.
3. Seleccione un perfil de Pasarela híbrida que ya no desee y pulse **Suprimir**.
   Después de confirmar que desea suprimir la Pasarela híbrida, el perfil se eliminará permanentemente.

Qué hacer a continuación

- Para eliminar de una aplicación cualquier sistema gestionado de agente híbrido en la Consola de Cloud APM, siga las instrucciones en "Gestión de aplicaciones" en la página 1133 para editar una aplicación.
- Si, en lugar de una eliminación correcta del software, obtiene un mensaje de error parecido al que se muestra en este ejemplo, revise el archivo de registro para conocer las causas posibles:

```
error: Failed dependencies:
ibm-java-x86_64-jre is needed by (installed) smai-kafka-00.08.00.00-1.el6.x86_64
La desinstalación ha fallado. El desinstalador no ha podido eliminar algunos de los
componentes,
por favor, revise el
 archivo de registro ("/tmp/hybridgateway/logs/uninstall-hybridgateway-20150228080551.log")
para obtener más información.
```

  El error que se muestra en el ejemplo se ha producido porque ibm-java-x86_64-jre es necesario para un paquete instalado externamente en el sistema. El instalador no elimina el JRE debido a que podría hacer que el otro paquete no funcionara. Como método alternativo, desinstale los productos con dependencia de ibm-java-x86-64-jre antes de desinstalar la Pasarela híbrida.

Gestión de la Pasarela híbrida

Utilice los comandos disponibles para el servicio de IBM Cloud Application Performance Management Hybrid Gateway para iniciarla o detenerla, comprobar el estado, desinstalar la Pasarela híbrida, y recopilar los archivos de registro si así se lo indica el servicio de soporte de IBM.

Acerca de esta tarea

Estos pasos presuponen que el directorio de instalación de la Pasarela híbrida es `/opt/ibm/`. En el sistema en el que está instalada la Pasarela híbrida, realice cualquiera de los pasos siguientes desde el indicador de mandatos:

Procedimiento

- Para iniciar el servicio de la Pasarela híbrida, especifique **/opt/ibm/hybridgateway/bin/hybridgateway.sh start**.
- Para detener el servicio de la Pasarela híbrida, especifique **/opt/ibm/hybridgateway/bin/hybridgateway.sh stop**.
- Para comprobar el estado de la Pasarela híbrida, especifique **/opt/ibm/hybridgateway/bin/hybridgateway.sh status**.
- Para desinstalar la Pasarela híbrida, especifique **/opt/ibm/hybridgateway/bin/hybridgateway.sh uninstall**.

  Vea también "Desinstalación de la Pasarela híbrida" en la página 996.
- Para comprobar los archivos de registro de la Pasarela híbrida, vaya a `/opt/ibm/wlp/usr/servers/hybridgateway/logs`.
- Para recopilar los archivos de registro de la Pasarela híbrida para el soporte de IBM, ejecute **/opt/ibm/hybridgateway/collectLogs.sh**.

  Se recopilan los archivos de registro y un mensaje muestra la ubicación de los archivos de registro comprimidos y le solicita que los envíe al soporte de IBM.

Gestor de Pasarela híbrida

Configure IBM Cloud Application Performance Management Hybrid Gateway para visualizar los datos de supervisión del dominio de IBM Tivoli Monitoring en la Consola de Cloud APM. Puede crear un perfil de Pasarela híbrida para cada Tivoli Enterprise Monitoring Server concentrador del entorno.

Después de pulsar **Configuración del sistema** > **Gestor de Pasarela híbrida**, se visualiza la página con una lista de las Pasarelas híbridas definidas.

La página contiene una tabla de todas las pasarelas híbridas configuradas para sus dominios de Tivoli Monitoring y tiene herramientas para gestionar los perfiles de Pasarela híbrida:

- **Añadir** abre la ventana **Añadir pasarela híbrida** para dar nombre al perfil nuevo. Después de especificar un nombre y pulsar **Añadir**, se abre la ventana **Editar pasarela híbrida**.
- Seleccione una pasarela híbrida y pulse **Editar** para abrir la ventana **Editar pasarela híbrida**.
- Seleccione una pasarela híbrida que ya no desee y pulse **Suprimir**. Después de confirmar que desea suprimir la pasarela híbrida, el perfil se eliminará permanentemente.
- Pulse una cabecera de columna para ordenar la tabla según esa columna; Control + clic en otra columna para añadir una clasificación secundaria.
- Pulse dentro del recuadro de texto de filtro y escriba el principio del valor por el que va filtrar. A medida que escribe, las filas que no coincidan con los criterios se filtrarán. Para borrar el filtro, pulse en el cuadro de filtro o pulse la tecla de retroceso.

Los campos obligatorios que debe rellenar para configurar la Pasarela híbrida están marcadas con un asterisco (*) en la ventana **Editar pasarela híbrida**.

Nombre de perfil
El nombre dado para el perfil de Pasarela híbrida que puede tener un máximo de 128 letras, números y signos de subrayado (_).

El nombre de perfil se solicita durante la instalación de Pasarela híbrida. Si ya ha instalado la Pasarela híbrida en el dominio de Tivoli Monitoring, utilice el nombre proporcionado o aceptado durante la instalación de la Pasarela híbrida.

Versiones más antiguas de la Pasarela híbrida no utilizan un perfil con nombre para acceder a sus datos de configuración. Si ha instalado la Pasarela híbrida antes del release de Cloud APM de Agosto de 2017, tiene un nombre de perfil especial, sin nombre (en blanco). Solo una versión más antigua de la Pasarela híbrida puede conectar con el Servidor de Cloud APM. Si configuró la Pasarela híbrida de versión anterior, el perfil si nombre muestra los valores configurados. Si no configuró la Pasarela híbrida de versión anterior, el perfil sin nombre muestra los valores predeterminados. Puede conservar el perfil sin nombre o suprimirlo y volver a añadirlo posteriormente según sea necesario y solo se puede utilizar para la versión Marzo 2017 (o anterior) de la Pasarela híbrida.

Nombre de grupo de sistemas gestionados
El grupo de sistemas gestionados de Tivoli Enterprise Portal Server que ha creado para ver los agentes de supervisión soportados en la Consola de Cloud APM. Los tipos de agente de supervisión que no están soportados por la oferta Cloud APM no se muestran en la consola independientemente de su inclusión en el grupo de sistemas gestionados.
Para obtener orientación e información sobre las limitaciones al crear el grupo de sistemas gestionados para habilitación híbrida, consulte .

Nombre de host de servidor de portal
Dirección IP o nombre de dominio completo del host de Tivoli Enterprise Portal Server.

Puerto de Portal Server
Número de puerto utilizado por Tivoli Enterprise Portal Server para las comunicaciones. El puerto predeterminado es `15200` para HTTP o `15201` para HTTPS. Un valor de 0 establece el puerto en el valor predeterminado `15200` para HTTP o `15201` para HTTPS.

Protocolo de Portal Server
Determina si se utiliza el protocolo de Internet HTTP o el protocolo seguro HTTPS para conectar con Tivoli Enterprise Portal Server. Valor predeterminado: `http`.

Nombre de usuario de Portal Server
El nombre de usuario para iniciar el cliente de Tivoli Enterprise Portal. Este ID de usuario debe tener acceso a todos los tipos de agente de supervisión (**Aplicaciones permitidas** se establece en **Todas las aplicaciones**). Para obtener más información, consulte Administrar usuarios en el Tivoli Monitoring Knowledge Center.

Contraseña de usuario de Portal Server
Contraseña asociada al nombre de usuario utilizado para iniciar la sesión en Tivoli Enterprise Portal.

Nombre de host de proxy de paso a través
Se utiliza si Tivoli Enterprise Portal Server se comunica mediante un servidor proxy de paso a través. Especifique la dirección IP o el nombre completo del sistema host de proxy.

Puerto de proxy de paso a través
Se utiliza si Tivoli Enterprise Portal Server se comunica mediante un servidor proxy de paso a través. Especifique el número de puerto para comunicarse con el proxy.

Protocolo de proxy de paso a través
Se utiliza si Tivoli Enterprise Portal Server se comunica mediante un servidor proxy de paso a través. Especifique el protocolo utilizado para las comunicaciones a través de proxy.Valor predeterminado: `http`.

Los agentes de Tivoli Monitoring que está viendo en la Consola de Cloud APM están en el entorno de IBM Tivoli Monitoring. Puede verlos en las páginas de Panel de instrumentos del rendimiento de aplicaciones, pero no puede crear umbrales para esos agentes en el **Gestor de umbrales**.

Integración con OMEGAMON

Puede visualizar datos y sucesos de los componentes de la aplicación OMEGAMON en la Consola de Cloud APM adquiriendo z Systems Extension Pack y utilizando la Pasarela híbrida para conectar uno o varios agentes de OMEGAMON desplegados a Cloud APM.

Antes de empezar

- Para utilizar z Systems Extension Pack, debe tener la oferta IBM Cloud Application Performance Management, Advanced o IBM Cloud Application Performance Management, Base.
- Debe haber uno o más agentes de OMEGAMON con licencia en ejecución en los LPAR de z Systems que se estén supervisando.
- Los agentes de OMEGAMON se conectan a la infraestructura de IBM Tivoli Monitoring.

Para obtener una lista de los agentes de OMEGAMON que puede visualizar en la Consola de Cloud APM, consulte el tema Cómo empezar correspondiente a su release en el temario IBM OMEGAMON for Application Performance Management de IBM Knowledge Center.

Procedimiento

Para integrar OMEGAMON con Cloud APM, siga estos pasos:

1. Después de añadir z Systems Extension Pack al producto Cloud APM, realice las siguientes tareas de la Pasarela híbrida:
   a) Instale la Pasarela híbrida.
   b) Cree el grupo de sistemas gestionados que desea visualizar en la Consola de Cloud APM.
   c) Configure la Pasarela híbrida en la Consola de Cloud APM para poder conectar la Pasarela híbrida a Tivoli Enterprise Portal Server y especificar un grupo de sistemas gestionados.

   Para obtener más información, consulte los temas adecuados de la sección “Pasarela híbrida” en la página 987.
2. Para ver el estado de las aplicaciones en el panel de instrumentos, inicie la sesión en la Consola de Cloud APM desde su navegador. Para obtener más información, consulte “Inicio de la Consola de Cloud APM” en la página 1009.

Integración con Netcool/OMNIbus

Puede reenviar los sucesos desde IBM Cloud Application Performance Management a su gestor de sucesos de IBM Tivoli Netcool/OMNIbus in situ.

Procedimiento

1. Para ver el Integration Agent for Netcool/OMNIbus y cómo se integra en Cloud APM con el Probe for Tivoli EIF para reenviar sucesos a Netcool/OMNIbus, consulte la configuración siguiente:

   El Integration Agent for Netcool/OMNIbus se conecta automáticamente con el servidor de Cloud APM. Esta conectividad permite que los sucesos fluyan del servidor a la red sin ninguna conexión de red de entrada.
2. Configure la integración para Netcool/OMNIbus.

Instalación y configuración del agente de integración para Netcool/OMNIbus

Para instalar Integration Agent for Netcool/OMNIbus, debe descargar un archivo de archivado desde el sitio web de IBM Marketplace, extraiga los archivos de instalación del agente y, después, inicie el script de instalación. Después de la instalación, el agente se inicia automáticamente, pero se debe configurar.

Acerca de esta tarea

Solo una instancia de Integration Agent for Netcool/OMNIbus puede reenviar sucesos de una sola instancia de una suscripción del servicio Cloud APM al gestor de sucesos Netcool/OMNIbus a la vez.

Procedimiento

1. Descargue el archivo de archivado de Cloud APM Integration que incluye el Integration Agent for Netcool/OMNIbus:
   a) Inicie la sesión con su cuenta y vaya a Productos y servicios en IBM Marketplace.
   b) Bajo **IBM Performance Management**, pulse **Más acciones**.
   c) Pulse **Mostrar paquetes adicionales**.
   d) Seleccione **IBM Performance Management OMNIbus Integration on Cloud**. Si es necesario, desplácese hacia abajo para encontrar este elemento.
   e) Pulse **Descargar**.
2. Guarde el archivo en el directorio intermedio de su elección. Instale el agente en los sistemas que tengan conectividad de red con Tivoli Netcool/OMNIbus Probe for Tivoli Event Integration Facility (EIF). Si fuera necesario, transfiera el archivo de archivado de instalación a los sistemas por supervisar. El archivo de archivado contiene el agente y el script de instalación.
3. Extraiga el archivo de instalación:

   Linux

   a. Abra una sesión en el shell de terminal en el sistema de Red Hat Enterprise Linux.

b. Vaya al directorio donde se encuentra el archivo de archivado.

c. Extraiga los archivos de instalación utilizando el mandato siguiente:

```
tar -xf ./apm_integration_agents_xlinux_8.1.4.0.tar
```

Windows

Extraiga el archivo `apm_integration_agents_win_8.1.4.0.zip`.

El script de instalación se extrae en un directorio especificado para el archivo de archivado y la versión. Por ejemplo, `IPM_Agent_Install_8.1.3.2`. El archivo binario del agente y los archivos relacionados con la configuración se extraen en los subdirectorios dentro de este directorio.

4. Ejecute el script de instalación con privilegios de administrador desde el directorio especificado para el archivo de archivado y versión.

   Si va a instalar Integration Agent for Netcool/OMNIbus en el mismo sistema en el que se encuentra Probe for Tivoli EIF y Probe for Tivoli EIF utiliza el puerto predeterminado 9998, Integration Agent for Netcool/OMNIbus se configura automáticamente para conectarse a Probe for Tivoli EIF.

   Importante: Si está instalando Integration Agent for Netcool/OMNIbus en un sistema que es diferente del sistema donde se encuentra Probe for Tivoli EIF, o si está utilizando un número de puerto que es diferente del predeterminado para Probe for Tivoli EIF, debe configurar Integration Agent for Netcool/OMNIbus una vez que se haya completado la instalación.

   Complete los pasos siguientes para instalar el agente:

   Linux `installAPMAgents.sh`

   Windows `installAPMAgents.bat`

   Se le solicitará que instale el Integration Agent for Netcool/OMNIbus.

   Se inicia una exploración de requisitos previos de su entorno y tarda varios minutos en completarse. Si faltan algunos requisitos, un mensaje le dirigirá a un archivo de registro que contiene la causa del error. La falta de un requisito previo, como por ejemplo la falta de una biblioteca o espacio de disco insuficiente detendrá la instalación. Debe identificar el error y volver a iniciar la instalación.

   El agente se configura con los siguientes valores predeterminados:

   ```
   Host del analizador EIF de Tivoli: localhost
   Puerto del analizador EIF de Tivoli: 9998
   ```

   Tras la instalación el Integration Agent for Netcool/OMNIbus se iniciará automáticamente.

   El agente de supervisión se instala en el directorio que especifique (*dir_instalación*). Se utilizan los directorios siguientes predeterminados:

   Linux `/opt/ibm/apm/agent`

   Windows `C:\IBM\APM\`

5. Si va a instalar Integration Agent for Netcool/OMNIbus en un sistema distinto de aquel donde se encuentra Probe for Tivoli EIF, o si Probe for Tivoli EIF utiliza un número de puerto distinto del puerto predeterminado 9998, Integration Agent for Netcool/OMNIbus debe estar configurado para conectarse a Probe for Tivoli EIF.

   Nota: si ha instalado Integration Agent for Netcool/OMNIbus en el mismo sistema en el que se encuentra Probe for Tivoli EIF y Probe for Tivoli EIF utiliza el puerto predeterminado 9998, no es necesario que complete este paso.

   Linux Complete los pasos siguientes para configurar el agente:

   a. Ejecute el mandato siguiente:

   ```
   dir_instalación/bin/omnibus-agent.sh config
   ```

   b. Cuando se le solicite, proporcione el nombre de host y número de puerto de Probe for Tivoli EIF.

Cuando se haya completado la configuración, el Integration Agent for Netcool/OMNIbus se iniciará automáticamente.

Linux O bien, puede utilizar los pasos siguientes para revisar y cambiar los valores de configuración.

a. Abra el archivo de respuestas *dir_instalación*/samples/omnibus_silent_config.txt en un editor de texto.
b. Edite el archivo para establecer o modificar los valores de configuración. Asegúrese de que elimina el comentario de las líneas de configuración.
c. Guarde y cierre el archivo de respuestas.
d. Configure de nuevo el agente. Ejecute el mandato siguiente, especificando la vía de acceso completa al archivo de configuración silenciosa que ha editado:

```
dir_instalación/bin/omnibus-agent.sh config dir_instalación/samples/
omnibus_silent_config.txt
```

e. Reinicie el agente para implementar los cambios:

```
dir_instalación/bin/omnibus-agent.sh stop
dir_instalación/bin/omnibus-agent.sh start
```

Windows Complete los pasos siguientes para configurar el agente:

a. Abra el archivo de respuestas *dir_instalación*\samples\omnibus_silent_config.txt en un editor de texto.
b. Edite el archivo para especificar el nombre de host y número de puerto de Probe for Tivoli EIF. Asegúrese de que elimina el comentario de las líneas de configuración.
c. Guarde y cierre el archivo de respuestas.
d. Vuelva a configurar el agente especificando la vía de acceso completa al archivo de configuración silenciosa que ha editado:

```
dir_instalación\BIN\omnibus-agent.bat config dir_instalación\samples
\omnibus_silent_config.txt
```

e. Reinicie el agente para implementar los cambios:

```
dir_instalación\BIN\omnibus-agent.bat stop
dir_instalación\BIN\omnibus-agent.bat start
```

Qué hacer a continuación

Siga las instrucciones de Configuración de la integración para Netcool/OMNIbus.

Si desea dejar de utilizar el Integration Agent for Netcool/OMNIbus o desea mover el agente a otro sistema, desinstale el agente mediante este mandato:

Linux *dir_instalación*/bin/omnibus-agent.sh uninstall
Windows *dir_instalación*\BIN\omnibus-agent.bat uninstall

Configuración de la integración para Netcool/OMNIbus

Tras instalar Integration Agent for Netcool/OMNIbus , debe copiar las reglas de suceso en Probe for Tivoli EIF y modificarlas. También debe actualizar Netcool/OMNIbus ObjectServer y el esquema de base de datos.

Antes de empezar

Antes de completar los pasos de integración, detenga Integration Agent for Netcool/OMNIbus mediante estos mandatos:

Linux *dir_instalación*/bin/omnibus-agent.sh stop

Windows *dir_instalación*\BIN\omnibus-agent.bat stop

dir_instalación es el directorio /opt/IBM/apm/agent o C:\IBM\APM predeterminado o el directorio que ha especificado durante la instalación de Integration Agent for Netcool/OMNIbus.

Acerca de esta tarea

Tras la instalación del Integration Agent for Netcool/OMNIbus, los siguientes archivos de configuración están en los directorios *dir_instalación*/localconfig/i0/omnibus y *dir_instalación* \localconfig\i0\omnibus:

- itm_apm_db_update.sql
- itm_event.rules
- itm_apm_event.rules

donde *dir_instalación* es el directorio /opt/IBM/apm/agent o C:\IBM\APM predeterminado o el directorio que ha especificado durante la instalación de Integration Agent for Netcool/OMNIbus.

Importante: Debe completar estos pasos, aunque Probe for Tivoli EIF y el servidor de objetos Netcool/OMNIbus ya estén integrados con IBM Tivoli Monitoring, Probe for Tivoli EIF, IBM SmartCloud Monitoring - Application Insight, IBM SmartCloud Application Performance Management, o una versión anterior de Cloud APM.

Procedimiento

En este procedimiento, cuando siga los enlaces a la documentación de IBM Tivoli Monitoring, complete solo los pasos proporcionados en la página enlazada.

1. Copie los archivos Integration Agent for Netcool/OMNIbus itm_event.rules y itm_apm_event.rules en el directorio de instalación de Probe for Tivoli EIF.

   Los siguientes directorios son los directorios predeterminados:

   Linux *dir_instalación*/tivoli/netcool/omnibus/probes/linux2x86

   Windows *dir_instalación*\Tivoli\Netcool\omnibus\probes\win32

   Donde *dir_instalación* es el valor predeterminado.
2. Abra el archivo Probe for Tivoli EIF tivoli_eif.rules en un editor de texto y siga uno de estos pasos:
   - Si usted es un cliente de IBM Tivoli Monitoring existente y ya ha completado la integración de OMNIbus, añada esta línea al archivo itm_event.rules: include "itm_apm_event.rules".
   - Si aún no ha configurado la integración de OMNIbus, elimine el comentario de la línea que hace referencia al archivo itm_event.rules.

   Para ver los pasos detallados, consulte Actualización de los archivos de reglas del analizador EIF en la documentación de IBM Tivoli Monitoring.
3. Si está utilizando una solución OMNIbus de varias capas, complete todas las tareas tal como se describe en la sección Actualización del Netcool/OMNIbus ObjectServer con atributos, tablas y desencadenantes de IBM Tivoli Monitoring de la documentación de IBM Tivoli Monitoring.
4. Actualice el esquema de base de datos de Netcool/OMNIbus ObjectServer cargando el archivo itm_apm_db_update.sql en la base de datos:

   Linux

   ```
   $OMNIHOME/bin/nco_sql -user nombre_usuario -password contraseña
   -server nombre_servidor < itm_apm_db_update.sql
   ```

   Ejemplo:

```
$OMNIHOME/bin/nco_sql -user smadmin -password passw0rd -server NCOMS <
/tmp/apm/itm_apm_db_update.sql
```

Windows

```
itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U nombre_usuario
-P contraseña -S nombre_servidor
```

Ejemplo:

```
\temp\apm\itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U smadmin
-P passw0rd -S NCOMS
```

Se podrían visualizar los mensajes de error siguientes al ejecutar los scripts, pero son inofensivos:

- `El objeto existe` e `Intento de insertar fila duplicada`, si los scripts se han ejecutado anteriormente (por ejemplo, para la integración con una versión anterior de Cloud APM o con Tivoli Monitoring).
- `ERROR=Objeto no encontrado en la línea 4 de la sentencia"-- Una tabla de espacio de trabajo para la automatización de borrado de suceso de ITM..."` en o cerca de `itm_event_clear`.
- `ERROR=Objeto no encontrado en la línea 1 de la sentencia "delete from alerts.itm_problem_events;..."` en o cerca de `itm_problem_events`.
- `ERROR=Objeto no encontrado en la línea 1 de la sentencia "drop table alerts.itm_problem_events;..."` en o cerca de `itm_problem_events`.

5. Repita el paso 5 para que el archivo se cargue en el servidor de objetos dos veces para asegurarse de que todas las dependencias se han cargado correctamente.
6. Inicie (o reinicie) Probe for Tivoli EIF.
7. Reinicie Integration Agent for Netcool/OMNIbus mediante estos mandatos:

   Linux *dir_instalación*`/bin/omnibus-agent.sh start`

   Windows *dir_instalación*`\BIN\omnibus-agent.bat start`

Integración con Operations Analytics - Log Analysis

Si su entorno incluye IBM Operations Analytics - Log Analysis, puede integrarlo para habilitar la búsqueda a través de registros de aplicación en Consola de Cloud APM.

Acerca de esta tarea

La integración con la aplicación Log Analysis instalada implica configurar el Servidor de Cloud APM con el URL. Para obtener más información sobre Log Analysis, consulte IBM Operations Analytics - Developers Community.

Debe proporcionar el URL de nivel superior para su instalación de análisis de registros, por ejemplo:

```
https://loganalysis.example.com:9987/Unity
```

El URL de análisis de registros debe ser accesible desde los hosts donde los usuarios trabajan con la Consola de Cloud APM. No es necesario que sea accesible desde internet abierto.

Procedimiento

1. En la Consola de Cloud APM, pulse **Configuración del sistema** > **Configuración avanzada**.
2. Seleccione la categoría **Integración de IU**.
3. En el campo **URL de análisis de registro**, entre el URL que se utiliza para iniciar la aplicación Log Analysis.

Resultados
La aplicación Log Analysis se integra y la función se habilita para que pueda buscar a través de registros de aplicación desde Panel de instrumentos del rendimiento de aplicaciones.

Nota:

El inicio de sesión único no está soportada desde Consola de Cloud APM en la aplicación Log Analysis.

Qué hacer a continuación
Seleccione **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** . Opcionalmente, seleccione una aplicación y, a continuación, utilice el cuadro de búsqueda para buscar en archivos de registro. De forma predeterminada, se busca en las entradas de la última hora, pero puede cambiar este periodo de tiempo. Si selecciona una aplicación, solo se busca en los registros en servidores asociados con esta aplicación. Para obtener instrucciones detalladas, consulte "Buscar en archivos de registro" en la página 1115.

Integración con Operations Analytics - Predictive Insights

Cuando integra IBM Cloud Application Performance Management con Operations Analytics - Predictive Insights, Operations Analytics - Predictive Insights analiza los datos de medida recopilados por Cloud APM y genera alarmas cuando identifica anomalías en los datos.

Las anomalías se visualizan como sucesos en los paneles de instrumentos de Cloud APM, tal como se describe en "Investigación de anomalías con Operations Analytics - Predictive Insights" en la página 1146. A continuación, puede descender a mayor nivel de detalle a la interfaz de usuario de Operations Analytics - Predictive Insights para ver más detalles sobre una anomalía.

Al añadir Operations Analytics - Predictive Insights a una suscripción de Cloud APM, se configura automáticamente para recopilar y analizar métricas de rendimiento. No es necesario configurar nada más. Para añadir Operations Analytics - Predictive Insights a una suscripción de Cloud APM, vaya a IBM Support y abra una petición de servicio.

Puede integrar los siguientes agentes de Cloud APM con Operations Analytics - Predictive Insights:

- Monitoring Agent for Db2
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for JBoss
- Monitoring Agent for Linux OS
- Monitoring Agent for Oracle Database
- Agente de Supervisión de tiempo de respuesta
- Monitoring Agent for UNIX OS
- Monitoring Agent for VMware VI
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ
- Monitoring Agent for Windows OS
- Monitoring Agent for Tomcat

Integración con Alert Notification

Para obtener más flexibilidad más allá del reenvío de correo electrónico básico de Cloud APM, puede integrar con el producto Alert Notification para ampliar las prestaciones de Cloud APM para notificar a los usuarios cuando se producen problemas.

La integración con Alert Notification le proporciona un control granular sobre quién recibe notificaciones y cómo se reciben. Por ejemplo, cada usuario puede decidir si desean recibir correo electrónico, SMS o

buzón de voz. Las notificaciones también se pueden direccionar a Slack. Distintos usuarios pueden recibir distintos tipos de notificaciones en función de la hora del día, el día de la semana, etc. Cada usuario puede decidir qué tipos de alertas desea recibir. Por ejemplo, un administrador de base de datos solo querrá recibir alertas de base de datos cuya gravedad sea de aviso o superior.

Antes de empezar

Alert Notification se integra automáticamente en la suscripción y la suscripción de prueba de IBM Cloud Application Performance Management.

Acerca de esta tarea

Los sucesos se configuran automáticamente para enviarlos a Alert Notification. A continuación, puede crear políticas de notificación para la suscripción para determinar las alertas para los que desea recibir notificaciones.

Puede añadir las aplicaciones supervisadas a los grupos de recursos. Para cada grupo de recursos guardado, puede configurar una o varias direcciones de correo electrónico. Cuando el rendimiento de un sistema gestionado de un grupo sobrepasa un umbral, se envía una notificación de correo electrónico a las direcciones configuradas para el grupo.

Alert Notification envía una notificación de correo electrónico para cualesquiera sucesos que se abran en los sistemas gestionados asignados al grupo.

Procedimiento

Siga los pasos “1” en la página 1006 y “2” en la página 1006 para cualquier Grupos de recursos para el que desee direccionar alertas en función del grupo de recursos.

1. Si desea direccionar alertas en función de grupos de recursos, siga estos subpasos:
   a) En la Consola de Cloud APM, pulse **Configuración del sistema** > **Gestor de grupos de recursos**.
   b) Seleccione un grupo de recursos y pulse **Editar** para abrir el **Editor de grupos de recursos**.

      Importante: Debe guardar un grupo de recursos nuevo o editado antes de abrir Alert Notification. Después de guardar, el Editor de grupo de recursos se cierra y debe volver a abrirlo si desea seguir utilizándolo.

      Si no guarda, después de configurar la notificación de correo electrónico en el paso “2” en la página 1006 y volver al Editor de grupo de recursos, es posible que reciba un mensaje de error en el que se indique que no se permite la actualización síncrona.
2. Siga estos pasos para configurar la notificación de correo electrónico:
   a) En el Editor de grupo de recursos de la consola APM, pulse el URL **Configure la notificación de correo electrónico** para abrir la aplicación IBM Alert Notification en una pestaña o ventana de navegador nueva.

      Esta acción crea automáticamente una política nueva basada en el grupo de recursos seleccionado en el paso “1” en la página 1006.

      Atención: Si su navegador no permite las ventanas emergentes, se impide que la ventana Alert Notification se abra. Debe establecer el navegador para permitir que la ventana Alert Notification lo abra para configurar la notificación de correo electrónico para un grupo de recursos.
   b) En Alert Notification, configure usuarios y grupos y asocie sus direcciones de correo electrónico a grupos de recursos para recibir notificaciones de sucesos por correo electrónico.

      Puede configurar sus propias políticas y notificaciones de Alert Notification para el tipo de alertas que desee recibir. Por ejemplo, un administrador de Linux solo querrá recibir correo electrónico, mensajes SMS o mensajes de buzón de voz para todos los sistemas Linux. A continuación, puede que desee desactivar las alertas de gravedad alta que son críticas. Una política permite filtrar todos los sucesos generados por el agente del sistema operativo Linux. Para obtener información sobre

cómo utilizar el Editor de notificaciones en la aplicación Alert Notification, consulte Creación de políticas de notificación.

Qué hacer a continuación
Para obtener más información sobre Alert Notification, consulte la Documentación de IBM Alert Notification.

Integración con Control Desk

Puede configurar los sucesos de Cloud APM para abrir automáticamente tíquets en IBM Control Desk.

Acerca de esta tarea
Puede integrar IBM Cloud Application Performance Management mediante la versión local o la versión de nube de IBM Control Desk.

Procedimiento

Utilice uno de los procedimientos siguientes:

- Para abrir tíquets en su IBM Control Desk V 7.6 local, complete los pasos siguientes:
  1. Configure la cuenta de correo electrónico de IBM SmartCloud > Notes para Control Desk para utilizar un cliente de correo IMAP. Durante la configuración, debe asegurarse de seleccionar **Habilitar acceso IMAP ahora**. Para obtener más información, consulte Enabling IMAP access (Cómo habilitar el acceso a IMAP) en IBM Connections for Social Cloud Knowledge Center.
  2. En la Consola de Cloud APM, pulse **Configuración del sistema** > **Configuración avanzada** y a continuación establezca los parámetros siguientes:

     Direcciones de correo electrónico de destino
     Especifique la dirección de correo electrónico de Notes que se utiliza para crear tíquets de solicitud de servicio.

     Línea de asunto de correo electrónico
     Especifique una línea de asunto para el correo electrónico, por ejemplo, `Suceso PMaaS`.
  3. Vaya a Soporte de Marketplace. y seleccione **Service Request** para enviar una incidencia de soporte para completar la habilitación.

     Proporcione la información siguiente en el tíquet:

     – Dirección de correo electrónico de SmartCloud Notes

       Por ejemplo, `user@ibmserviceengage.com`.
     – Contraseña de correo electrónico de SmartCloud Notes
     – Nombre de servidor completo de SmartCloud Notes

       Por ejemplo, `imap.notes.na.collabserv.com`.
     – Número de puerto de correo electrónico de SmartCloud Notes

       Por ejemplo, 993.
     – URL de IBM Control Desk del cliente

       Ponga el enlace con este formato: `https://<id-suscriptor>.sccd.ibmserviceengage.com/maximo_t4hj/webclient/login/login.jsp?welcome=-true`
  4. Para configurar el escucha de correo electrónico para analizar el correo electrónico y manejarlo adecuadamente cuando desee asignar tíquets a otros grupos en IBM Control Desk on Cloud, consulte la sección Configuración de escuchas de correo electrónico.
- Para abrir tíquets en el entorno de nube IBM Control Desk, siga estos pasos:

1. Vaya a Soporte de Marketplace. y seleccione **Service Request** para enviar una incidencia de soporte para completar la habilitación.

   Proporcione la información siguiente en el tíquet:

   – Dirección de correo electrónico de SmartCloud Notes

     Por ejemplo, `user@ibmserviceengage.com`.

   – Contraseña de correo electrónico de SmartCloud Notes

   – Nombre de servidor completo de SmartCloud Notes

     Por ejemplo, `imap.notes.na.collabserv.com`.

   – Número de puerto de correo electrónico de SmartCloud Notes

     Por ejemplo, 993.

   – URL de IBM Control Desk del cliente

     Ponga el enlace con este formato: `https://<id-suscriptor>.sccd.ibmserviceengage.com/maximo_t4hj/webclient/login/login.jsp?welcome=-true`

2. Para configurar el escucha de correo electrónico para analizar el correo electrónico y manejarlo adecuadamente cuando desee asignar tíquets a otros grupos en IBM Control Desk on Cloud, consulte la sección Configuración de escuchas de correo electrónico.

Integración con IBM Cloud

Puede ver información de supervisión de sus aplicaciones dentro del entorno de IBM Cloud mediante los recopiladores de datos autónomos.

Cuando está configurado para recopilar datos de una aplicación IBM Cloud, un recopilador de datos habilita la integración de prestaciones de supervisión con IBM Cloud. Los recopiladores de datos transfieren datos de diagnóstico y supervisión de recursos sobre las aplicaciones IBM Cloud al Servidor de Cloud APM. El Servidor de Cloud APM recibe y procesa la información de supervisión recopilada por los recopiladores de datos. Pueden supervisarse los siguientes tipos de aplicaciones IBM Cloud:

- Aplicaciones Liberty
- Aplicaciones Node.js
- Aplicaciones Python
- Aplicaciones Ruby

Después de configurar adecuadamente un recopilador de datos, podrá ver los datos de supervisión en la Consola de Cloud APM. Para ver instrucciones de configuración, consulte “Procedimiento general para configurar recopiladores de datos” en la página 192.

Integración con IBM Agent Builder

Puede crear, modificar, depurar y empaquetar agentes utilizando Agent Builder que amplía las prestaciones de supervisión de un entorno de IBM Tivoli Monitoring o IBM Cloud Application Performance Management. Un agente personalizado utiliza cualquiera de estos entornos para supervisar cualquier tipo de software de desarrollo propio o personalizado.

Para conocer los detalles, consulte el documento IBM Agent Builder: Guía del usuario.

Capítulo 9. Administración

Inicio de la Consola de Cloud APM

Inicie la sesión en Consola de Cloud APM del navegador para revisar el estado de salud de las aplicaciones en los paneles de instrumentos.

Antes de empezar

- Active la cuenta mediante el enlace que se proporciona en el correo electrónico de confirmación que ha recibido después del registro inicial en el servicio.
- Para asegurarse de que la interfaz de usuario no está truncada, utilice una resolución mínima de 1280 x 1024.
- Para optimizar el rendimiento, use uno de los navegadores soportados. Para obtener una lista de los navegadores soportados, vaya a System requirements (APM Developer Center). Seleccione uno de los enlaces del producto IBM Cloud Application Performance Management y pulse el enlace "Server"; en el informe que se visualiza, pulse o desplácese a "Web Browsers".

Procedimiento

1. Para acceder a la Consola de Cloud APM, utilice el enlace que se proporciona en el correo electrónico que le informa de que el servicio está preparado.
2. También puede acceder a la consola desde el sitio web IBM Marketplace:
   a. Vaya a Productos y servicios en el sitio web de IBM Marketplace.
   b. Inicie la sesión con el nombre de usuario y la contraseña que ha utilizado para registrarse en el servicio.
   c. En la fila Servidor de Cloud APM, haga clic en **Iniciar**.

Resultados

Después de iniciar la sesión, se visualiza la página **Cómo empezar** con opciones de aprendizaje para **Tareas de usuario** y **Tareas del administrador** y enlaces a **Recursos de la comunidad**.

Qué hacer a continuación

- Familiarícese con los elementos de interfaz de usuario pulsando el enlace de hipertexto para realizar una visita guiada del panel de instrumentos de Cloud APM. Vea los vídeos de las tareas de usuario y administrador, que le ayudarán a dar los primeros pasos en la utilización y personalización del entorno de Cloud APM.
- Añada aplicaciones para ver paneles de instrumentos de los recursos en agrupaciones lógicas, como por ejemplo Pedido en línea. Encontrará instrucciones en: “Gestión de aplicaciones” en la página 1133.
- Cree umbrales para probar las condiciones que, cuando se cumplen, hacen que se abra un suceso. Por ejemplo, puede tener un umbral que abra un suceso una vez la capacidad de almacenamiento alcance el 90%. Para obtener instrucciones, consulte “Gestor de umbrales” en la página 1019.
- Añada y asigne usuarios a grupos de usuarios y roles para controlar el acceso a las características de la Consola de Cloud APM y a los recursos gestionados. Para obtener más información, consulte el apartado “Gestión del acceso de usuarios” en la página 1035.
- Para obtener más información sobre la supervisión de IBM Pila de aplicaciones Java y Pila de integración de IBM, consulte “Escenarios” en la página 92.

- Si, en lugar de ir a la página Guía de inicio o al Panel de instrumentos del rendimiento de aplicaciones, el navegador fuera al sitio web de IBM, significaría que su ID de usuario carece de permisos para acceder a la Consola de Cloud APM. Deberá solicitar acceso al administrador.
- Si no se muestra ninguna métrica para un origen de datos, consulte Foro de Cloud Application Performance Management en developerWorks. Busque el foro para el "panel de instrumentos", conteste a una entrada para realizar una pregunta relacionada o cree una nueva entrada y describa el síntoma.
- Si está iniciando la Consola de Cloud APM en Internet Explorer 8, 9 o 10 y obtiene un error `Esta página no se puede visualizar`, es posible que tenga que habilitar la opción de seguridad, TLS 1.2. Para obtener más información, vaya a Foro de Cloud Application Performance Management y busque "tls".

Umbrales y grupos de recursos

Los umbrales prueban determinadas condiciones, como por ejemplo, número de transacciones por minuto menor de 100, y abren un suceso cuando se cumplen las condiciones. Utilice umbrales para supervisar problemas reales y potenciales con los recursos supervisados. Asigne umbrales a grupos de recursos para supervisar en todos los sistemas gestionados del mismo tipo que pertenecen al grupo.

Información básica

Revise la información básica para aprender sobre los umbrales, los umbrales predefinidos para sus agentes, los grupos de recursos a los que se han asignado y la personalización de umbrales.

Umbrales predefinidos

Los agentes de supervisión vienen con *umbrales predefinidos* que están habilitados y se inician con el agente. La primera vez que abre el **Gestor de umbrales** después de la instalación del agente, los umbrales que se listan para el tipo de origen de datos seleccionado son los umbrales predefinidos. Estos umbrales predefinidos están asignados al grupo de recursos del sistema por omisión para el agente y se muestran en la columna **Grupos asignados**.

Si edita un umbral predefinido, como por ejemplo para cambiar el nombre o condición, el umbral ya no se trata como un umbral predefinido, sino que se considera un *Umbral personalizado*. Sin embargo, puede cambiar el grupo de recursos asignado para un umbral predefinido del grupo de sistemas predeterminado a un grupo definido por el usuario y sigue siendo un umbral predefinido.

Si prefiere no utilizar los umbrales predefinidos, puede desactivarlos en la página **Configuración avanzada** (consulte “Habilitación de umbrales” en la página 1110). La inhabilitación de los umbrales predefinidos no los elimina del **Gestor de umbrales**; sólo se elimina su asignación de grupo, dejándolos inactivos. Después de inhabilitar los umbrales predefinidos, puede abrir el **Gestor de umbrales** y ver que la columna **Grupos asignados** está vacía para cada umbral predefinido (consulte “Ejemplos de umbrales inhabilitados” en la página 1012).

Puede habilitar el umbral como un umbral personalizado asignándolo a cualquier grupo de recursos disponible.

Umbrales personalizados

Los umbrales nuevos que crea son umbrales personalizados, tal como se indica en la columna de **Gestor de umbrales Origen**. Si edita un umbral predefinido, también se convierte en un umbral personalizado y su origen cambia de "Predefinido" a "Personalizado".

Ejecutar mandato

Cuando se abre un suceso para un umbral que se evalúa en true, puede hacer que se ejecute automáticamente un mandato o script de mandatos en el sistema supervisado para el que se ha abierto el suceso. Por ejemplo, podría desear registrar información, desencadenar un pitido audible o detener un trabajo que utiliza demasiados recursos.

El mandato utiliza esta sintaxis:

```
&{conjunto_datos.atributo}
```

donde *conjunto_datos* es el nombre del conjunto de datos y *atributo* es el nombre del atributo tal como se muestra en el Editor de umbrales. Si el conjunto de datos o el nombre del atributo contiene un espacio, sustitúyalo por un signo de subrayado.

El ejemplo siguiente muestra cómo puede pasar el parámetro de nombre de disco al recurso gestionado.

```
/scripts/clean_logs.sh &{KLZ_Disk.Disk_Name}
```

Puede pasar uno o varios atributos del conjunto de datos. Si se especifica, se pasan por orden varios atributos en el mandato ($1, $2, etc.).

El mandato se ejecuta desde la línea de mandatos con la misma cuenta de usuario con la que se inició el agente. Por ejemplo, si el agente se ejecuta como root, entonces root ejecuta el mandato en el sistema gestionado.

Las opciones siguientes controlan la frecuencia con la que se ejecuta el mandato:

Seleccione ☐ **Sólo cuando se produce el primer suceso** si el conjunto de datos devuelve varias filas y desea ejecutar el mandato solo para la primera aparición del suceso en el ejemplo de datos. Quite la marca del recuadro de selección para ejecutar el mandato para cada fila que causa un suceso.

Seleccione ☐ **Para cada intervalo verdadero consecutivo** para ejecutar el mandato cada vez que el umbral se evalúa como verdadero. Quite la marca del recuadro de selección para ejecutar el mandato cuando el umbral es true, pero no ejecutarlo de nuevo hasta que el umbral se evalúe en false, seguido por otra evaluación en true en un intervalo subsiguiente.

Grupos de recursos

Los grupos de recursos representan una colección de sistemas gestionados y controlan cómo se distribuyen los umbrales. Un umbral se asigna al grupo de recursos que incluye los sistemas gestionados donde desea que se ejecute.

Todos los umbrales predefinidos tienen una asignación de grupo de recursos predeterminado, que es el grupo definido por el sistema para el tipo de agente como, por ejemplo, Db2 y Microsoft IIS.

Puede crear grupos de recursos personalizados y seleccionar los sistemas gestionados que se deben incluir en cada grupo. Puede tener varios tipos de agentes en un grupo de recursos personalizado; los umbrales que están asignados al grupo se distribuyen únicamente a los sistemas gestionados del mismo tipo de agente. Por ejemplo, un umbral que se crea con atributos del sistema operativo Linux y se asigna a un grupo de recursos del sistema operativo Linux, MongoDB y sistemas gestionados Python, sólo se distribuye a los sistemas gestionados del sistema operativo Linux.

Para obtener más información, consulte “Gestor de grupos de recursos” en la página 1014.

Estado de suceso de Panel de instrumentos del rendimiento de aplicaciones

Las gravedades de estado que se muestran en Panel de instrumentos del rendimiento de aplicaciones indican la gravedad de suceso más alta de la aplicación, grupo, subgrupo e instancia del sistema gestionado seleccionados.

Después de seleccionar una aplicación desde el navegador o desde un recuadro de resumen del panel de instrumentos **Todas mis aplicaciones**, un panel de instrumentos con pestañas presentará distintas facetas de su aplicación. La pestaña **Sucesos** proporciona información sobre los sucesos para el elemento de navegador seleccionado, tal como se describe en “Estado de suceso” en la página 1143.

Los cambios de umbral afectan a otros umbrales asignados al mismo agente de supervisión

Después de crear, modificar o suprimir una definición de umbral o cambiar la lista de umbrales que se distribuyen a un agente de supervisión, todos los sucesos muestreados se cierran para los agentes a los que se ha distribuido el umbral. Tras el cierre de suceso, los agentes de supervisión reabrirán las condiciones de umbral para sucesos que se evalúan como true. En la Consola de Cloud APM, los sucesos cerrados desaparecen de la consola hasta que se reabren con un nuevo valor **Indicación de fecha y hora**. Si está recibiendo notificaciones por correo electrónico para los sucesos, recibirá notificaciones por correo electrónico del cierre y de la apertura de sucesos.

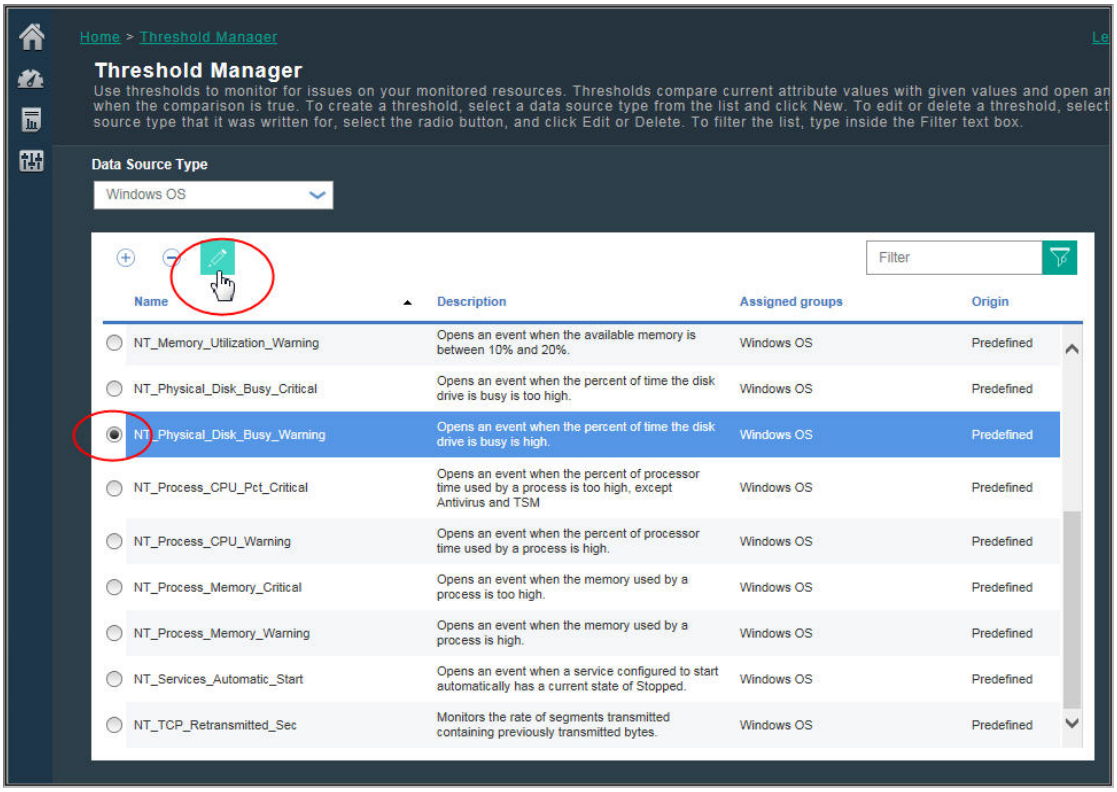
Por ejemplo, piense que tiene un grupo de recursos personalizado denominado Sistemas de sitio con el sistema operativo Linux y que se han asignado umbrales y agentes de WebSphere Applications. Cree un nuevo umbral del sistema operativo Linux y asígnelo a Sistemas de sitio. Todos los sucesos muestreados abiertos en los agentes del sistema operativo Linux asignados al sistema de sitios se cierran. A continuación, los sucesos muestreados se reabren si las condiciones de umbral siguen siendo verdaderas.

Ejemplos de umbrales inhabilitados

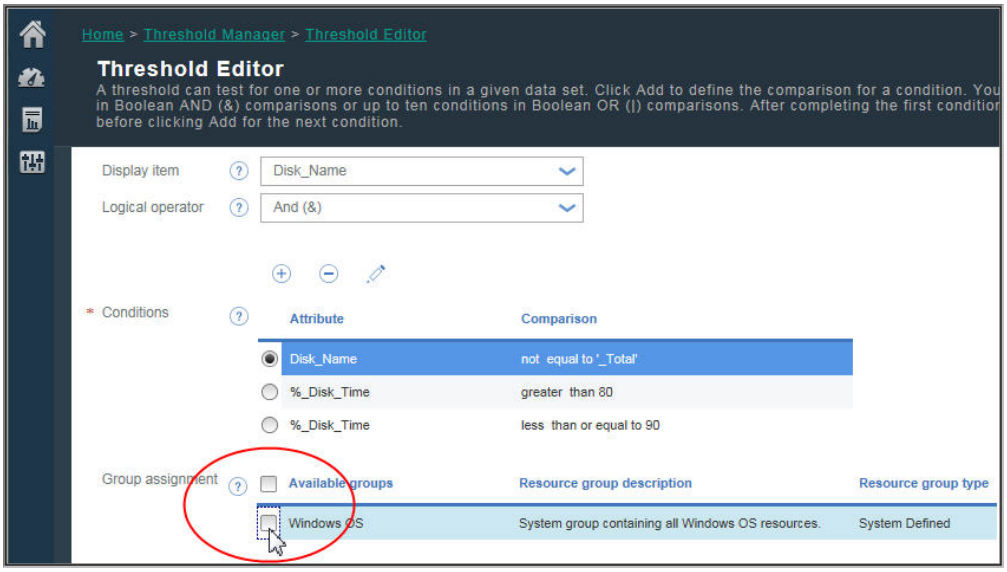
Puede inhabilitar los umbrales predefinidos para todos los agentes en el entorno. También puede inhabilitar umbrales individualmente, tanto predefinidos como personalizados. Cuando un umbral está inhabilitado, no se está ejecutando en sistemas gestionados y no se abren sucesos.Puede inhabilitar un umbral eliminando su asignación (o asignaciones) de grupo de recursos. También hay disponible un valor de **Configuración avanzada** para inhabilitar los umbrales predefinidos para todos los agentes.

Inhabilitación de un solo umbral

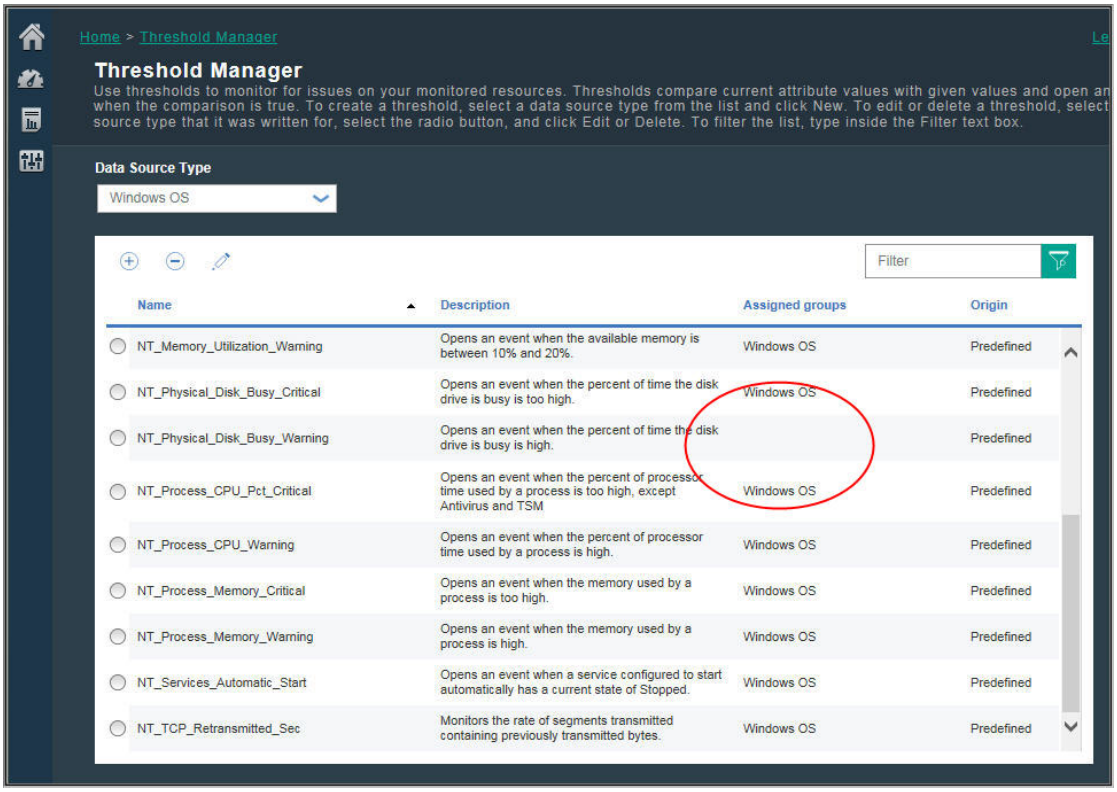
En esta imagen, el umbral para ser inhabilitado está seleccionado en el **Gestor de umbrales** y el usuario pulsa **Editar**:



El umbral se abre en el Editor de umbrales. El usuario deselecciona la casilla del grupo de recursos asignado en el campo **Asignación de grupos**:

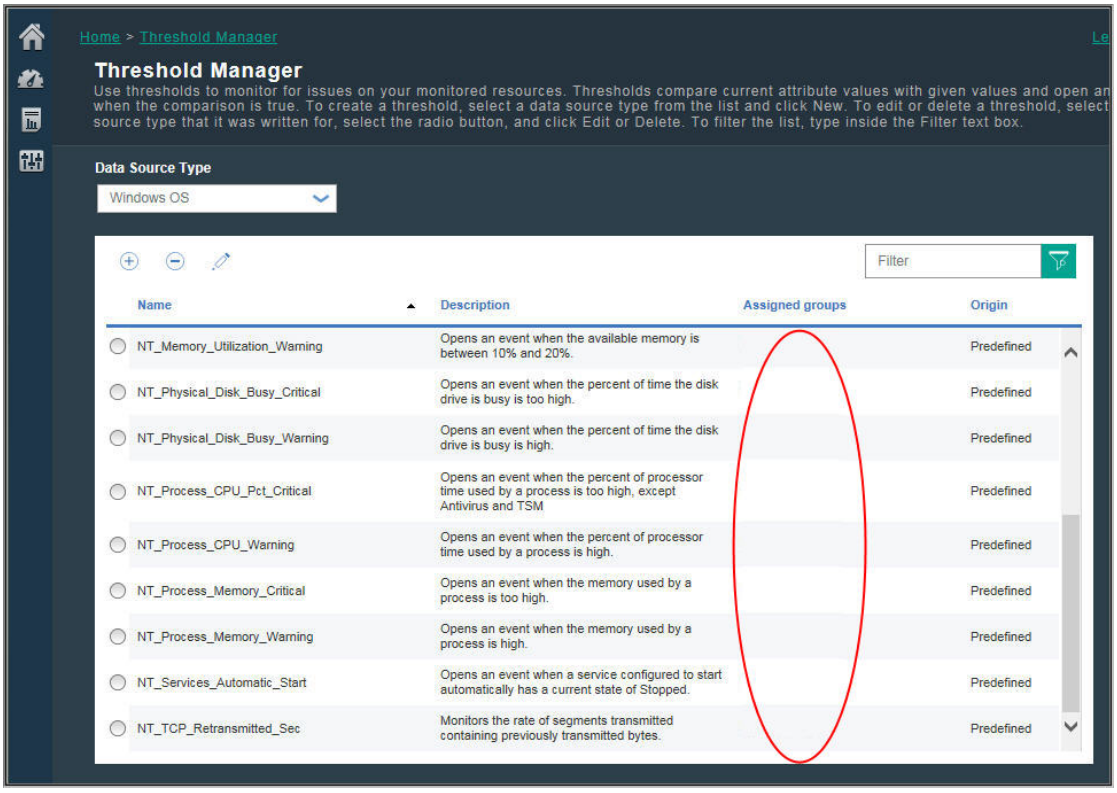


Cuando el usuario pulsa **Guardar**, se visualiza el **Gestor de umbrales**. El umbral se inhabilita y la columna **Grupos asignados** está vacía:



Inhabilitación de todos los umbrales predefinidos

Desactive todos los umbrales predefinidos para todos los agentes de supervisión en la página **Configuración avanzada**, tal como se describe en "Habilitación de umbrales" en la página 1110. La próxima vez que abra el **Gestor de umbrales**, la columna **Grupos asignados** está vacía para cada umbral predefinido, indicando que los umbrales están inactivos:



Conceptos relacionados

"Información básica" en la página 1010

Revise la información básica para aprender sobre los umbrales, los umbrales predefinidos para sus agentes, los grupos de recursos a los que se han asignado y la personalización de umbrales.

Referencia relacionada

"Gestor de umbrales" en la página 1019

Gestor de grupos de recursos

El entorno supervisado puede tener varios sistemas gestionados que se pueden clasificar de acuerdo con su finalidad. Dichos sistemas a menudo tienen los mismos requisitos de umbral. Utilice el **Gestor de grupos de recursos** para organizar sistemas supervisados en grupos a los que puede asignar umbrales. Puede crear también grupos de recursos que se correlacionan con las políticas de control de acceso basado en roles (RBAC).

Después de pulsar **Configuración del sistema** > **Gestor de grupos de recursos**, la página se abre con una tabla de grupos de recurso definidos. Inicialmente, se muestra un grupo de sistemas predefinido para cada tipo de agente de supervisión instalado, como `SO Windows`.. Cada grupo de sistemas contiene todos los umbrales predefinidos para el agente.

El acceso al **Gestor de grupos de recursos** y a los grupos de recursos se controla mediante los permisos de usuario. Debe tener permiso de visualización para un grupo de recursos para verlos; debe tener permisos de modificación para crear, editar o suprimir un grupo de recursos.

La tabla tiene herramientas para gestionar grupos de recursos:

- **Nuevo** abre el **Editor de grupos de recursos** para asignar sistemas gestionados y umbrales.
- Seleccione un grupo de recursos para ver los recursos asignados y los umbrales asignados al grupo en el panel adyacente.
- Seleccione un grupo de recursos y pulse **Editar** para abrir el **Editor de grupos de recursos** para cambiar el sistema gestionado y las asignaciones de umbral.

- Seleccione un grupo de recursos que ya no desee y pulse **Suprimir**. Después de confirmar la supresión, los umbrales que se habían asignado al grupo se deben asignar a otro grupo si desea que continúen ejecutándose en los sistemas gestionados.
- Puede pulsar dentro del cuadro de texto de filtro y teclear el valor por el que desea filtrar. A medida que escribe, las filas que no coincidan con los criterios se filtrarán. Para borrar el filtro, pulse en el cuadro de filtro o pulse la tecla de retroceso.

La tabla muestra los grupos de recursos disponibles:

Nombre de grupo de recursos
Los grupos predefinidos se denominan por su tipo de agente; los grupos personalizados se denominan por el autor.

Descripción del grupo de recursos
Un grupo predefinido se describe como un *grupo de sistemas* para el recurso supervisado; los grupos personalizados se describen según el autor.

Un grupo de sistemas, como S0 `Linux`, incluye todos los umbrales predefinidos para el agente y todos los sistemas gestionados donde está instalado el agente. Puede editar un grupo de sistemas para asignar o eliminar los umbrales pero no puede asignar ni eliminar los sistemas gestionados. Los sistemas gestionados se asignan automáticamente a un grupo de sistemas del mismo tipo, incluido cualquier del dominio de Tivoli Monitoring si tiene una Pasarela híbrida configurada.

Algunos recursos de sistema están relacionados con agentes que admiten subnodos. En función del tipo de agente, se pueden añadir los subnodos, el nodo de agente, o las dos cosas, a las aplicaciones. Si solo se pueden añadir los subnodos a las aplicaciones definidas, no podrá ver los sucesos para ninguno de los umbrales definidos para el nodo de agente. Sin embargo, se pueden reenviar los sucesos a un gestor de sucesos como Netcool/OMNIbus. Además, los suscriptores de IBM Cloud Application Performance Management pueden configurar Alert Notification.

Tipo de grupo de recursos
Los grupos predefinidos son de tipo *Definido por el sistema*. Tiene un grupo predefinido para cada tipo de agente instalado en el entorno.

Los grupos personalizados que usted u otros usuarios del entorno crean son de tipo *Definido por el usuario*.

Editor de grupo de recursos

Después de pulsar **Nuevo** para añadir un grupo o después de seleccionar un grupo y pulsar **Editar** para editar un grupo, el **Editor de grupos de recursos** se visualiza con los campos siguientes:

Nombre de grupo
El nombre del grupo es necesario. Puede cambiar un nombre de grupo personalizado existente y todas las referencias al grupo se actualizarán automáticamente después de guardar los cambios.

Descripción de grupo
Opcional para los grupos personalizados. Añada una descripción de la organización del grupo. La descripción se visualiza en el **Gestor de grupos de recursos**.

Asignación de recursos
Todos los sistemas gestionados que se pueden añadir al grupo se muestran en la lista de agentes por los nombres de sistema gestionado el nombre de host, el tipo de agente y su dominio. Puede pulsar una cabecera de columna para ordenar la lista según el nombre de agente, el nombre de host, el tipo o el dominio.

Para llenar el grupo, marque el recuadro de selección de uno o varios sistemas gestionados.

Puede seleccionar **Mostrar solo los recursos seleccionados** para ocultar los sistemas gestionados no asignados.

Si ha configurado la IBM Cloud Application Performance Management Hybrid Gateway, puede añadir los sistemas gestionados del dominio de IBM Tivoli Monitoring a los grupos de recursos definidos por el usuario. No puede añadir los sistemas gestionados de Tivoli Monitoring a los grupos definido por el sistema ni puede crear umbrales para ellos.

Asignación de umbral

Todos los umbrales que se han predefinido o añadido mediante el **Gestor de umbrales** se muestran en la lista de umbrales por su nombre y tipo de agente. Puede pulsar la cabecera de una columna para ordenar la lista.

Para añadir un umbral al grupo, marque el recuadro de selección situado junto al nombre. Para eliminar un umbral del grupo, deseleccione el recuadro de selección. Debe tener permiso de visualización para el **Gestor de umbrales** para añadir o eliminar umbrales. Al añadir umbrales a un grupo de sistemas, los umbrales disponibles se limitan a aquellos cuyo conjunto de datos es apto para el grupo de sistemas.

Los umbrales que ha asignado al grupo se distribuyen entre los sistemas gestionados en el grupo del mismo tipo de agente. Aunque puede asignar umbrales de cualquier tipo de agente de supervisión a un grupo, los umbrales asignados solo se distribuyen entre los sistemas gestionados del mismo tipo que son miembros del grupo. Por ejemplo, si asigna el umbral `MySQL_Process_Down` al grupo, se incluye en el grupo, pero se distribuye solo a los sistemas gestionados del Monitoring Agent for MySQL que pertenecen al grupo.

Puede seleccionar **Mostrar sólo los umbrales seleccionados** para ocultar los umbrales no asignados. Si va a filtrar la lista, pulse × del recuadro de filtro para borrar el filtro y habilitar el recuadro de selección.

También puede asignar un grupo de recursos a un umbral desde el **Gestor de umbrales**.

Configure la notificación de correo electrónico

Disponible con IBM Cloud Application Performance Management: pulse **Configurar notificación de correo electrónico** para abrir la aplicación IBM Alert Notification en una pestaña o una ventana de navegador nueva. Utilice Alert Notification para crear usuarios y asociar las direcciones de correo electrónico a los grupos de recursos para recibir notificaciones de sucesos por correo electrónico.

Atención: Si su navegador no permite las ventanas emergentes, se impide que la ventana Alert Notification se abra. Debe establecer el navegador para permitir que la ventana Alert Notification lo abra para configurar la notificación de correo electrónico para un grupo de recursos.

Después de pulsar **Guardar**, el grupo de recursos se guarda con la lista de grupos de recursos y se muestra en la tabla **Gestor de grupos de recursos**.

Tareas relacionadas

“Integración con Alert Notification” en la página 1005
“Exploración de las API” en la página 1107

Referencia relacionada

“Gestor de umbrales” en la página 1019

Guía de aprendizaje: Definición de un umbral

Los umbrales son el mecanismo de alerta de problemas reales y posibles problemas con los recursos gestionados. Utilice la guía de aprendizaje para aprender los pasos básicos para definir un umbral y generar una alarma cuando se produce la condición.

Acerca de esta tarea

Esta guía de aprendizaje utiliza el agente de sistema operativo Linux para mostrar cómo definir un umbral en el **Gestor de umbrales** y ver la alarma generada en el Panel de instrumentos del rendimiento de aplicaciones. El ID de usuario debe tener permiso de vista para que el **Gestor de umbrales** realice estos pasos.

Procedimiento

1. Desde la barra de navegación, pulse **Configuración del sistema** > **Gestor de umbrales**.
2. Pulse el recuadro de lista **Tipo de origen de datos** y seleccione el tipo de datos **SO Linux**.
   Se mostrarán en la tabla los umbrales definidos para el agente de sistema operativo Linux.

3. Pulse **Nuevo** para abrir el **Editor de umbrales** y definir el umbral.
4. Defina un umbral para generar una alarma de gravedad desconocida cuando el promedio de CPU esté por debajo del 75 %:
   a) En el campo **Nombre**, especifique `CPU_average_below_75_percent`.
   b) En el campo **Descripción**, especifique `Guía de aprendizaje de umbrales`
   c) Deje los campos **Gravedad**, **Intervalo** y **Muestras consecutivas obligatorias** en sus valores predeterminados.
   d) En el campo **Conjunto de datos**, seleccione **`Promedios de CPU de KLZ`**.
   e) En el campo **Condiciones**, pulse **Nuevo** y añada la comparación en el recuadro de diálogo emergente.
      1) En el campo **Atributo**, seleccione **`CPU_Usage_Current_Average`**
      2) En el campo **Operador**, seleccione **`Menor que`**
      3) En el campo **Valor**, especifique 75.

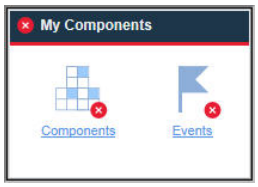
      Después de pulsar **Aceptar**, se mostrarán el atributo y la comparación en el campo **Condiciones**.
   f) En el campo **Asignación de grupos**, seleccione el grupo de sistemas **`SO Linux`**.
   g) Pulse **Guardar** para completar la definición y volver a la página **Gestor de umbrales**.

   Se mostrará `CPU_average_below_75_percent` en la lista de umbrales definidos para el origen de datos SO Linux.

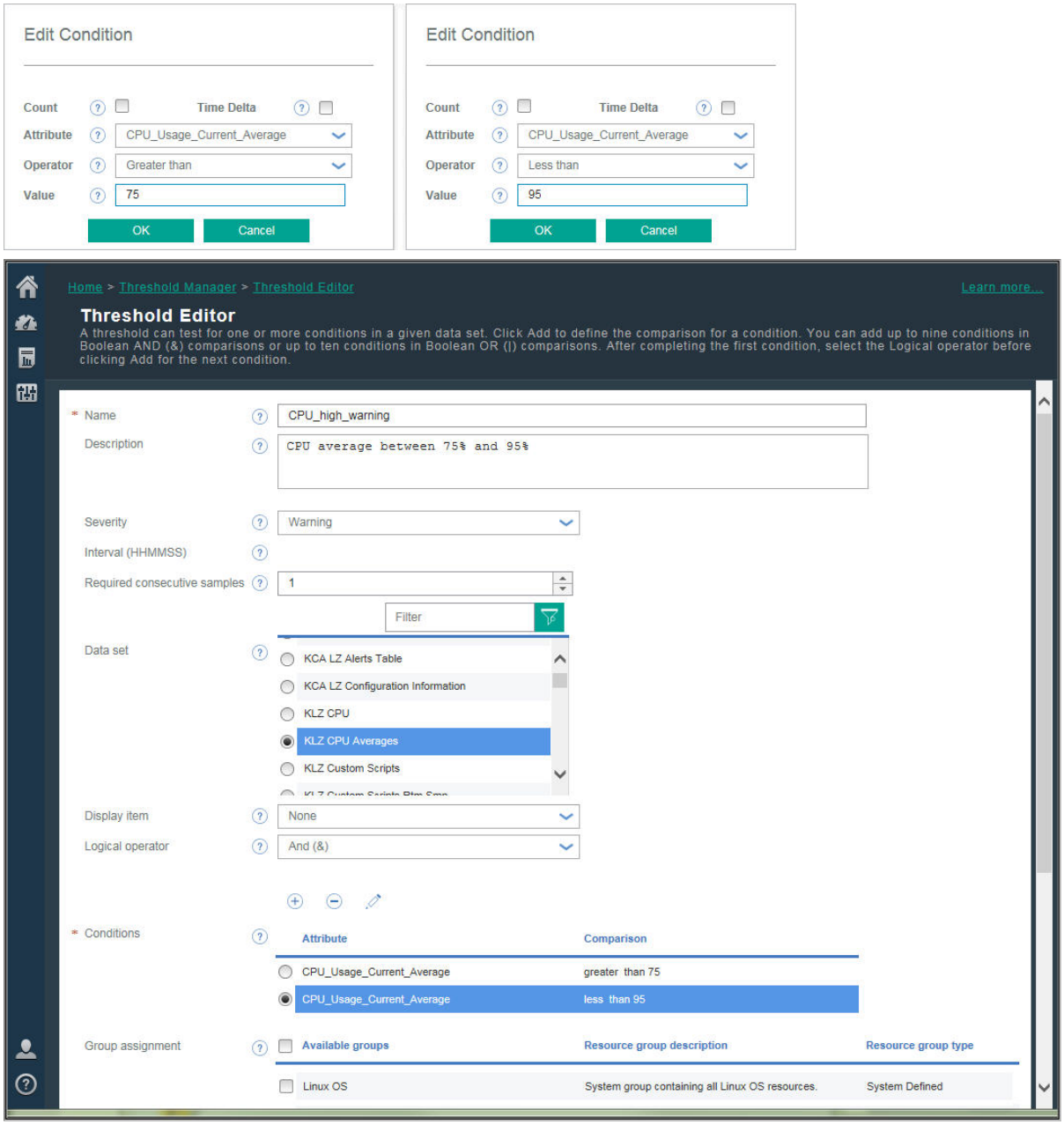
Resultados
Ha definido un umbral que genera una alarma cuando el uso de CPU en cualquiera de los sistemas gestionados del sistema operativo Linux está por debajo del 75 %.

Qué hacer a continuación

- Visualice el suceso:
  1. En la barra de navegación, pulse **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones**.
  2. En el recuadro de resumen **Mis componentes**, pulse el enlace **Sucesos**.

  3. En la pestaña **Sucesos** que se abre, busque el umbral `CPU_average_below_75_percent` en la lista. Puede llevar 1 o 2 minutos que se active la alarma. Sin embargo, si el promedio de CPU está por encima del 75 por ciento, no se activará la alarma.
- Edite el umbral:
  1. Desde la barra de navegación, pulse **Configuración del sistema** > **Gestor de umbrales**.
  2. Pulse el recuadro de lista **Tipo de origen de datos** y seleccione el tipo de datos **`SO Linux`**.
  3. Seleccione el umbral `CPU_average_below_75_percent` de la lista y pulse **Editar**.
  4. Cambie cualquiera de los campos para que se le avise de una condición que desee. Por ejemplo, podría cambiar **Nombre** a `CPU_high_warning`, cambiar **Gravedad** a **`Aviso`**, editar la condición para que sea **`Mayor que 75`** y añadir una condición: **`Menor que 95`**. Para editar la comparación, pulse **Editar**, cambie **Operador** a **`Mayor que`** y pulse **Aceptar**. Para añadir la nueva condición, deje el campo **Operador lógico** en el valor predeterminado **And (&)**, pulse **Nueva** para obtener una nueva condición, seleccione **Operador `Menor que`** y especifique **Valor** 95.



- Revise los umbrales predefinidos para los agentes y ajuste los valores de comparación como correspondan para su entorno.
- Cree nuevos umbrales para activar alarmas de otras condiciones de las que desea que se le avise.

Referencia relacionada

“Gestor de umbrales” en la página 1019

Guía de aprendizaje: Definición de un umbral para ejecutar un mandato en el recurso gestionado

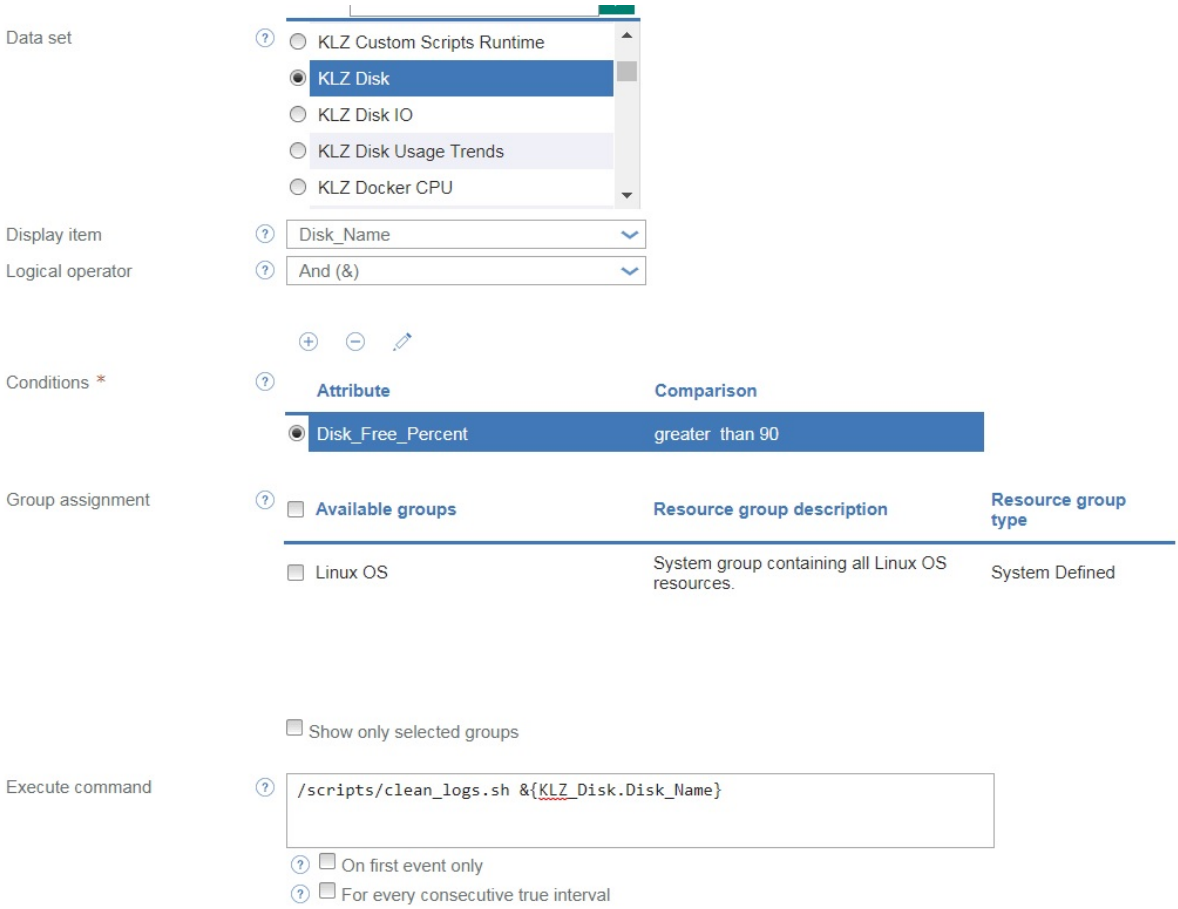
Puede utilizar el **Editor de umbrales** para pasar ciertos parámetros a los agentes. Puede especificar mandatos o un script de mandatos para que se ejecute automáticamente cuando se desencadena un suceso.

Acerca de esta tarea

Esta guía de aprendizaje muestra cómo utilizar el campo **Ejecutar mandato** para pasar un parámetro al agente de IBM Cloud Application Performance Management.

Procedimiento

1. Abra el **Gestor de umbrales** seleccionando **Configuración del sistema** > **Gestor de umbrales**.
2. Seleccione *SO Linux* en el campo **Tipo de origen de datos**.
   Se mostrarán en la tabla los umbrales definidos para el agente de sistema operativo Linux.
3. Pulse **Nuevo** para abrir el **Editor de umbrales** y definir el umbral.
4. Defina el umbral y las condiciones especificando valores para los diferentes parámetros, como por ejemplo **Nombre**, **Gravedad** y **Condiciones**.
5. Seleccione *KLZ Disk* en el campo **Conjunto de datos**.



6. Especifique el mandato siguiente en el campo **Ejecutar mandato**:

```
/scripts/clean_logs.sh &{KLZ_Disk.Disk_Name}
```

   Debe sustituir el espacio en el conjunto de datos *KLZ Disk* por un signo de subrayado.
   KLZ_Disk.Disk_Name se pasa al script de mandatos

Resultados
El script de mandatos se configura para ejecutarse automáticamente para el umbral definido. Los mandatos se ejecutan en el sistema supervisado para el que se desencadenan los sucesos.
Referencia relacionada
"Gestor de umbrales" en la página 1019

Gestor de umbrales

Utilice el **Gestor de umbrales** para revisar los umbrales predefinidos para un agente de supervisión y para crear y editar umbrales.Los umbrales se utilizan para comparar el valor muestreado de un atributo con el valor establecido en el umbral. Si el valor muestreado satisface la comparación, se abre un suceso. El suceso se cierra automáticamente cuando la comparación del umbral ya no es verdadera (true).

Después de pulsar **Configuración del sistema** > **Gestor de umbrales**, la página se visualiza con una tabla de los umbrales definidos para el tipo del origen de datos seleccionado.

Los tipos de datos que se muestran cuando pulsa el cuadro de lista **Tipo de origen de datos** son de los tipos de agentes de supervisión y recopiladores de datos que están instalados en el entorno gestionado. Seleccione el tipo de datos en el que desea crear o ver umbrales.

La tabla lista todos los umbrales que se han creado para el tipo de datos seleccionado y tiene herramientas para gestionar umbrales:

- **Nuevo** abre el **Editor de umbrales** para definir un umbral para el tipo de datos seleccionado.
- Seleccione un umbral y pulse **Editar** para abrir el **Editor de umbrales** para editar la definición.
- Seleccione un umbral que ya no desee y pulse **Suprimir**. Después de confirmar que desea suprimir el umbral, se elimina de la lista y de los grupos de recursos a los que se había asignado. Los sucesos abiertos para el umbral se cierran.
- Para obtener una lista larga, puede pulsar dentro del cuadro de texto de filtro y teclear el principio del valor por el que desea filtrar. A medida que escribe, las filas que no coincidan con los criterios se filtrarán. Para borrar el filtro, pulse × en el cuadro de filtro o pulse la tecla de retroceso.

Para obtener más información sobre los umbrales predefinidos y los umbrales personalizados que se muestran en la tabla y el significado de la asignación de grupo de recursos (o falta de los mismos), consulte "Información básica" en la página 1010. Para obtener una lección práctica rápida, consulte "Guía de aprendizaje: Definición de un umbral" en la página 1016.

Editor de umbrales

Después de pulsar **Nuevo** o seleccionar un umbral y pulsar **Editar**, aparece el Editor de umbrales con los siguientes campos:

Nombre
: Escriba un nombre exclusivo para el umbral. El nombre debe empezar por una letra y puede tener hasta 31 letras, números y signos de subrayado, como por ejemplo "Aviso_veloc_procesador_promedio". El nombre de umbral se visualiza en el separador Panel de instrumentos del rendimiento de aplicaciones **Sucesos** y en determinadas tablas del panel de instrumentos.

Descripción
: Opcional. Una descripción es útil para registrar la finalidad del umbral, que los usuarios pueden ver en el **Gestor de umbrales**.

Gravedad
: Seleccione la gravedad del suceso adecuada de la lista: Muy grave, Crítico, Leve, Aviso, o Desconocido.

  Las gravedades se consolidad para su visualización en Panel de instrumentos del rendimiento de aplicaciones: los sucesos Crítico y Muy grave se muestran como ; los sucesos Leve y Aviso se muestran como ; y los sucesos Desconocidos se muestran como (consulte "Estado de suceso" en la página 1143).

¿Reenviar suceso EIF?
: Si ha configurado el reenvío de sucesos en la página **Configuración del sistema** > **Configuración avanzada** ("Gestor de sucesos" en la página 1108), de forma predeterminada se reenvían sucesos abiertos a destinos de sucesos que ha configurado, por ejemplo, destinos de sucesos EIF, Cloud Event Management o Alert Notification. Cambie el valor a **No** si no desea reenviar sucesos para este umbral a todos los destinos de sucesos.

  Si ha configurado el reenvío de sucesos en la página de **Configuración del sistema** > **Configuración avanzada** (Gestor de sucesos), los sucesos abiertos se reenvían a un receptor EIF de forma predeterminada. Cambie el valor a **No** si no desea reenviar sucesos para este umbral a un receptor EIF.

Para personalizar cómo se correlacionan los umbrales con los sucesos reenviados, alterando temporalmente la correlación predeterminada entre los umbrales y los sucesos reenviados al servidor de sucesos, pulse **Personalización de atributo EIF**. Para obtener más información, consulte "Personalización de un suceso para reenviarlo a un receptor EIF" en la página 1025.

Intervalo
Especifique o seleccione el tiempo de espera entre la toma de muestras de datos en el formato *HHMMSS*, como por ejemplo 00 15 00 para 15 minutos. Para umbrales de sucesos de muestra, el intervalo mínimo es 000030 (30 segundos) y el máximo es 235959 (23 horas, 59 minutos y 59 segundos).

Un valor de 000000 (seis ceros) indica un umbral de *suceso puro*. Los sucesos puros son notificaciones no solicitadas. Los umbrales para sucesos puros no tienen ningún intervalo de muestreo, por lo que no tienen ninguna medida constante que se pueda supervisar para valores actuales. Los sucesos puros se cierran después de 24 horas o tal como se establece en la página **Configuración avanzada** en el campo **Hora de cierre de sucesos puros** en la categoría "Gestor de sucesos" en la página 1108.

Muestras consecutivas obligatorias
Especifique cuántas muestras de umbral consecutivas deben evaluarse en true para que se genere un suceso: para cualquier umbral con un valor de 1 y una muestra que se evalúa en true, se genera inmediatamente un suceso; un valor de 2 significa que se deben evaluar en true dos muestras de umbral consecutivas para que se abra un suceso.

Conjunto de datos
Seleccione el conjunto de datos (grupo de atributos) para el tipo de datos que se pueda muestrear. Los atributos disponibles para su inclusión en la condición se seleccionan del conjunto de datos escogido. Si el umbral tiene varias condiciones, todas deben ser el mismo conjunto de datos.

Para obtener una descripción abreviada de un conjunto de datos, pase el puntero del ratón sobre el nombre. Puede obtener la descripción completa del conjunto de datos y los atributos pulsando el enlace "Obtener más información" en la ayuda contextual. También puede pulsar **Ayuda** > **Contenido de la ayuda** o **Ayuda** > **Documentación** en la barra de navegación y abrir la ayuda o descargar la referencia para el agente de supervisión.

Algunos agentes se clasifican por categorías como agentes de varios nodos, que tienen subnodos para supervisar varios recursos de agentes. Un agente de varios nodos puede tener conjuntos de datos que pueden utilizarse en un umbral pero cualquier suceso abierto para el umbral no se visualiza en los Panel de instrumentos del rendimiento de aplicaciones. Un mensaje le notificará la limitación. Dichos sucesos pueden reenviarse al gestor de sucesos de IBM Netcool/OMNIbus.

Elemento de visualización
Opcional. Sólo para conjuntos de datos de varias filas. Después de que una evaluación de fila haga que se abra un suceso, no se pueden abrir más sucesos para este umbral en el sistema supervisado hasta que se cierra el suceso. Si selecciona un elemento de visualización, habilita el umbral para continuar evaluando las otras filas del muestreo de datos y abrir más sucesos si otras filas cumplen la condición. Además, el elemento de visualización se muestra en la pestaña **Sucesos** del Panel de instrumentos del rendimiento de aplicaciones para que pueda distinguir fácilmente entre las filas para las cuales se han abierto sucesos. La lista sólo contiene los atributos que puede designar como elementos de visualización.

Operador lógico
Ignore este campo si su umbral solo tiene una condición. Si está midiendo varias condiciones, seleccione uno de los operadores siguientes antes de pulsar **Nuevo** para añadir una segunda (o tercera, etc.) condición:

And (&) si la condición anterior y la condición siguiente se deben cumplir para que se llegue al umbral
Or (|) si se puede cumplir cualquiera de ellas para llegar al umbral

No se admite una mezcla de operadores lógicos; utilice los operadores And u Or. El umbral puede tener hasta un máximo de nueve de condiciones cuando se utiliza el operador Or; un máximo de 10 de condiciones cuando se utiliza el operador And.

Si está utilizando la función `Missing` (descrita posteriormente en la sección **Operador**), solo puede utilizar el operador And en la fórmula.

Condiciones

La definición de umbral puede incluir de forma lógica varios umbrales o condiciones a la vez.

Pulse **Nuevo** para añadir una condición. Seleccione una condición y pulse **Editar** para modificar la expresión o pulse **Suprimir** para eliminar la expresión.

Después de pulsar **Nuevo** o **Editar**, complete los campos en el cuadro de diálogo **Añadir condición** o **Editar condición** que se abre:

Recuento

Para los conjuntos de datos que devuelven varias filas para cada muestra de datos puede contabilizar cada fila que cumple los criterios de la condición. Un suceso se abre una vez que se ha alcanzado el recuento **Valor** y se cumplen las demás condiciones de la fórmula. Por ejemplo, si el número de procesos "zombie" pasa de 10, se debe emitir una alerta.

En el ejemplo siguiente, la condición se cumple cuando se han contado más de 10 filas: **Atributo** Indicación de fecha y hora, **Operador** Mayor que, , **Valor** 10.

Marque el recuadro de selección **Recuento**, el **Atributo** a contar, el **Operador** relacional y el **Valor** de recuento.

Si la fórmula tiene varias condiciones, cada condición debe utilizar el operador booleano **And**. **Recuento** y **Delta de tiempo** son mutuamente excluyentes: si marca el recuadro de selección para una función, la otra función está inhabilitada. El atributo no puede ser un identificador del sistema como por ejemplo Nombre de servidor u ORIGINNODE, especificarse como **Elemento de visualización** o ser de un conjunto de datos para el que el umbral abre sucesos puros.

Delta de tiempo

Utilice la función **Delta de tiempo** en una condición para comparar la indicación de fecha y hora de muestreo (como por ejemplo el tiempo de registro) con la diferencia de tiempo especificada.

Después de marcar el recuadro de selección **Delta de tiempo**, el campo Delta de tiempo se visualiza para que combine + (más) o - (menos) con el número de días, horas, minutos o segundos. Seleccione **Hora de muestreo** u **Hora específica** con el valor a utilizar en la comparación.

En el siguiente ejemplo de registro de sucesos, la fórmula compara la hora en que el suceso se ha registrado con la indicación de fecha y hora del muestreo de datos. Si el suceso se produjo siete días antes, la comparación será verdadera. Si el operador relacional se cambió a Menor o igual que, la comparación será verdadera después 8 días, 9 días, etc:

Atributo Indicación de fecha y hora
Delta de tiempo -7 días
Operador Igual
Valor Hora de entrada

Atributo

Seleccione el atributo que desee comparar en esta condición. Para ver una breve descripción del atributo, pase el puntero del ratón sobre el nombre en la lista.

Operador

Seleccione el operador relacional para el tipo de comparación:

```
Igual a
No igual a
Mayor que
Mayor o igual a
```

Menor que
Menor o igual que
La expresión regular contiene
La expresión regular no contiene

`La expresión regular contiene` y `La expresión regular no contiene` buscan una coincidencia de patrón de la expresión. Cuanto más fácil sea la coincidencia de una serie con la expresión, más eficiente será la carga en el agente. La expresión no tiene que coincidir con la línea entera; solamente la subserie en la expresión. Por ejemplo, en `Ver la película`, desea saber si la serie contiene `la`. Puede crear la expresión regular utilizando `la`, pero también podría utilizar `.*la.*`. O bien, si busca `Ver`, puede especificar `Ver` o puede especificar `^Ver` para confirmar que está al principio de la línea. Especificar comodines `.*` genera una búsqueda menos eficiente y aumenta la carga de trabajo. Para obtener más información sobre las expresiones regulares, consulte el tema biblioteca técnica developerWorks® o busque `regex` en el navegador.

También puede seleccionar la función `Missing`, que compara el valor de la métrica especificada con una lista de valores que proporcione. La condición es verdadera si el valor no coincide con ninguno de la lista. Esta función es útil si desea recibir una notificación cuando falte algo en el sistema. Requisitos y restricciones:

1. La métrica seleccionada debe ser un atributo de texto: los atributos numéricos y de texto no se pueden utilizar.
2. Separe cada valor con una coma (,), por ejemplo, `fred,mary,jean`.
3. Solo puede tener una condición `Missing` en un umbral.
4. `Missing` debe ser la última condición de la fórmula. Si son necesarias otras condiciones, especifíquelas antes de añadir la función Missing y utilice solo el operador **And (&)** en la fórmula. De lo contrario, todas las filas subsiguientes se inhabilitarán.

Valor
Escriba el valor que se debe comparar con el formato que está permitido para la métrica, como por ejemplo 20 para el 20% o 120 para 2 minutos.

Asignación de grupos
Asigne un grupo de recursos para distribuir el umbral a los sistemas gestionados del mismo tipo existentes en el grupo de recursos. Los grupos de recursos que están disponibles son los grupos definidos por el usuario que tiene permiso para Modificar y los grupos del sistema (para el tipo de agente) que tiene permiso para ver. Los grupos del sistema disponibles también están limitados a aquellos que son adecuados para el conjunto de datos elegido.

Un umbral sin ningún grupo asignado no se distribuye a ningún sistema supervisado y permanece detenido hasta que se distribuye a un grupo de recursos.

Un grupo de sistemas, como `Linux OS` o `HTTP Server`, distribuye el umbral a todos los sistemas gestionados en los que está instalado el agente. De forma predeterminada, cada umbral predefinido se asigna al grupo de sistemas para ese agente. (Puede inhabilitar todos los umbrales predefinidos en la página **Configuración avanzada**, tal como se describe en “Habilitación de umbrales” en la página 1110.)

La excepción son los sistemas gestionados del dominio de IBM Tivoli Monitoring: los sistemas gestionados del dominio de Tivoli Monitoring deben ser supervisados con situaciones que se han distribuido en el entorno de Tivoli Monitoring.

Para asignar grupos al umbral, marque el recuadro de selección de uno o varios grupos de recursos. Si la lista de grupos asignados es larga, puede seleccionar **Mostrar solo los grupos seleccionados**.

Si no ve un grupo de recursos al que desea asignar el umbral, puede guardar la definición de umbral y pulsar **Aceptar** cuando se le solicite que confirme si desea guardar el umbral sin asignarlo a un grupo. A continuación podrá crear un nuevo grupo en **Gestor de grupos de recursos** y asignar un umbral a un nuevo grupo en el **Editor de grupo de recursos**. Para obtener más información, consulte “Gestor de grupos de recursos” en la página 1014.

Ejecutar mandato

Cuando se abre un suceso para un umbral que se evalúa en true, puede hacer que se ejecute automáticamente un mandato o script de mandatos en el sistema supervisado para el que se ha abierto el suceso. Por ejemplo, podría desear registrar información, desencadenar un pitido audible o detener un trabajo que utiliza demasiados recursos.

El mandato utiliza esta sintaxis:

```
&{conjunto_datos.atributo}
```

donde *conjunto_datos* es el nombre del conjunto de datos y *atributo* es el nombre del atributo tal como se muestra en el Editor de umbrales. Si el conjunto de datos o el nombre del atributo contiene un espacio, sustitúyalo por un signo de subrayado.

El ejemplo siguiente muestra cómo puede pasar el parámetro de nombre de disco al recurso gestionado.

```
/scripts/clean_logs.sh &{KLZ_Disk.Disk_Name}
```

Puede pasar uno o varios atributos del conjunto de datos. Si se especifica, se pasan por orden varios atributos en el mandato ($1, $2, etc.).

El mandato se ejecuta desde la línea de mandatos con la misma cuenta de usuario con la que se inició el agente. Por ejemplo, si el agente se ejecuta como root, entonces root ejecuta el mandato en el sistema gestionado.

Las opciones siguientes controlan la frecuencia con la que se ejecuta el mandato:

Seleccione ☐ **Sólo cuando se produce el primer suceso** si el conjunto de datos devuelve varias filas y desea ejecutar el mandato solo para la primera aparición del suceso en el ejemplo de datos. Quite la marca del recuadro de selección para ejecutar el mandato para cada fila que causa un suceso.

Seleccione ☐ **Para cada intervalo verdadero consecutivo** para ejecutar el mandato cada vez que el umbral se evalúa como verdadero. Quite la marca del recuadro de selección para ejecutar el mandato cuando el umbral es true, pero no ejecutarlo de nuevo hasta que el umbral se evalúe en false, seguido por otra evaluación en true en un intervalo subsiguiente.

Después de pulsar **Guardar**, el umbral se aplica a todos los sistemas supervisados del mismo tipo de datos dentro de los grupos de recursos asignados.

Consejo: Puede controlar el comportamiento de sucesos y el reenvío de sucesos a través de las opciones del **Gestor de sucesos** en la página **Configuración avanzada**. Consulte “Configuración avanzada” en la página 1108.

Nota: Para ver una lista de los atributos que son adecuados para su inclusión en la definición del umbral, cree una tabla con el conjunto de datos que tiene previsto utilizar. .

Conceptos relacionados

“Información básica” en la página 1010
Revise la información básica para aprender sobre los umbrales, los umbrales predefinidos para sus agentes, los grupos de recursos a los que se han asignado y la personalización de umbrales.

Tareas relacionadas

“Guía de aprendizaje: Definición de un umbral” en la página 1016

“Guía de aprendizaje: Definición de un umbral para ejecutar un mandato en el recurso gestionado” en la página 1018
Puede utilizar el **Editor de umbrales** para pasar ciertos parámetros a los agentes. Puede especificar mandatos o un script de mandatos para que se ejecute automáticamente cuando se desencadena un suceso.

“Integración con Netcool/OMNIbus” en la página 999
Puede reenviar los sucesos desde IBM Cloud Application Performance Management a su gestor de sucesos de IBM Tivoli Netcool/OMNIbus in situ.

Personalización de un suceso para reenviarlo a un receptor EIF

Puede personalizar los sucesos de umbral que se envían a un receptor EIF (Event Integration Facility o recurso de integración de sucesos), como por ejemplo Netcool/OMNIbus ObjectServer, a Cloud Event Management o Alert Notification. Utilice la ventana **Personalización de atributo EIF** para personalizar el contenido de suceso que se reenvía a los destinos de sucesos, alterando temporalmente la correlación predeterminada. Puede crear definiciones de correlación para sucesos de umbral enviados al receptor del recurso de integración de sucesos (EIF). Utilice la ventana **Personalización de atributo EIF** para personalizar cómo se correlacionan los sucesos de umbral con los sucesos EIF reenviados, alterando temporalmente la correlación predeterminada. Mediante la personalización de la plantilla de mensaje, puede añadir información sobre el problema identificado por el suceso y datos específicos del suceso. Mediante la personalización de la plantilla de mensaje, puede añadir información sobre el problema identificado por el suceso e incluir datos específicos del suceso.

Acerca de esta tarea

Puede personalizar el atributo base EIF, que es un atributo **msg** predefinido que envía la fórmula de umbral a un destino de sucesos. También puede añadir uno o más atributos personalizados EIF al suceso. Si utiliza Netcool/OMNIbus ObjectServer, debe actualizar el archivo de reglas de analizador EIF y los desencadenantes de ObjectServer si desea ver los atributos personalizados en la interfaz de usuario de Netcool/OMNIbus.

Puede personalizar el atributo base EIF, que es un atributo **msg** predefinido que envía la fórmula de umbral al receptor EIF. También puede añadir uno o más atributos personalizados EIF lo que requiere una actualización del receptor EIF y el archivo de reglas del análisis.

Procedimiento

Siga estos pasos para personalizar la forma en que los sucesos del umbral actual se correlacionan con los sucesos reenviados:

1. Si el **Gestor de umbrales** no está abierto, pulse **Configuración del sistema** > **Gestor de umbrales**.
2. Pulse el recuadro de lista **Tipo de origen de datos** y seleccione el tipo de datos con el que desee trabar.
3. Si este es un nuevo umbral, pulse **Nuevo**; de lo contrario, seleccione un umbral y pulse **Editar**.
4. Para personalizar cómo se correlacionan los sucesos para este umbral con los sucesos reenviados, asegúrese de que **Reenviador EIF** esté establecido en Sí, pulse **Personalización de atributo EIF** y realice uno de los pasos siguientes:
   - **Atributos base EIF**: para personalizar el atributo base, pulse el botón de selección para **msg** y pulse **Editar**.
   - **Atributos personalizados EIF**: para personalizar un atributo personalizado, pulse **Añadir**; para editar un atributo personalizado, pulse el botón de selección correspondiente al atributo y pulse **Editar**.

   Se abrirá la ventana **Editar atributo** o **Añadir atributo**.
5. Complete los campos para personalizar los valores de atributo:

Campo	Descripción	Restricción
Nombre de atributo	Nombre del atributo personalizado EIF, que debe empezar con un carácter.	El atributo base EIF es **msg** y no se puede cambiar.
Tipo de atributo	El tipo de atributo personalizado EIF: **Tipo de serie** o **Tipo de número**.	El atributo base EIF es **Tipo serie** y no se puede cambiar.
Subtipo	El valor asignado al atributo, correspondiente al tipo de atributo:	Un atributo **Tipo de número** sólo puede utilizar

Campo	Descripción	Restricción
	• **`Atributo personalizado`** habilita el campo **Atributo personalizado** para añadir el valor del atributo personalizado cuando que se produce el suceso. • **`Valor literal`** habilita el campo **Valor literal** para añadir texto a la plantilla de mensaje. • **`Valor literal + Atributo correlacionado`** habilita los campos **Valor literal** y **Atributo correlacionado** para añadir valores de texto y atributo a la plantilla de mensaje, y habilita el botón **Añadir** para añadir varios valores de texto o atributo (o ambos). Se añade un espacio tras cada valor literal o atributo. El uso típico del atributo base EIF **`msg`** especifica un **`Valor literal + Atributo correlacionado`** para la plantilla de mensaje.	**`Atributo correlacionado`**.
Añadir	Si desea enviar varios valores literales o valores de atributo en el mensaje reenviado, pulse **Añadir** para añadir otro conjunto de campos **Valor literal** y **Atributo correlacionado**. Cada vez que selecciona **Añadir**, estos campos se añaden al panel. Para eliminar un conjunto de campos **Valor literal** y **Atributo correlacionado**, deseleccione ambos campos antes de pulsar **Aceptar**. Consulte Ejemplo.	Sólo está habilitado cuando **Subtipo** es **`Valor literal + Atributo correlacionado`**. Máximo de 6 conjuntos de campos **Valor literal** y **Atributo correlacionado**. Si no puede ver los campos que ha añadido, utilice la característica de zoom del navegador (Ctrl -) para reducir el diseño de forma que se ajuste al recuadro de diálogo.
Valor literal	El texto que se incluirá en la plantilla de mensaje. Por ejemplo, un valor literal de `La utilización de memoria es alta con un` con el atributo correlacionado **`%Memory Utilization`** se muestra en la interfaz de usuario **Gestor de sucesos** como `Memory Utilization is high at 97.3%` (La utilización de memoria es alta con un 97,3%). La plantilla de mensaje consta de texto de mensaje fijo y referencias de sustitución de variables, o símbolos. El símbolo hace referencia a datos de atributo de suceso o comunes o una referencia especial a la fórmula de umbral. Los atributos comunes son los atributos incluidos en todos los sucesos reenviados, como *nombre_umbral*; los atributos de suceso son aquellos atributos que son específicos del `msg` de umbral.	Está inhabilitado cuando **Subtipo** es **`Atributo correlacionado`**.
Atributo correlacionado	El atributo cuyo valor desea añadir a la plantilla de mensaje. Los atributos disponibles son del conjunto de datos que se ha seleccionado para el umbral. Por ejemplo, para un umbral que supervisa el tiempo de procesador elevado, es posible que desee	Máximo de 6 campos **Atributo correlacionado**. Inhabilitado cuando **Subtipo** es **`Valor literal`**.

Campo	Descripción	Restricción
	correlacionar el atributo el porcentaje de tiempo de usuario.	Cuando el **Tipo de atributo** es **`Tipo de número`**, sólo están disponibles atributos numéricos.
Multiplicador	El multiplicador es el valor definido tras personalizar el valor del número del atributo correlacionado original con un multiplicador: valor de atributo = *atributo1* * *n*. Por ejemplo, si desea convertir minutos a segundos en el suceso EIF, especifique el multiplicador 60. El valor del multiplicador puede ser una fracción, expresada como decimal, como por ejemplo 0,5 o 5.4.	Sólo está habilitado para atributos numéricos (**Tipo de atributo** es **`Tipo de número`**).

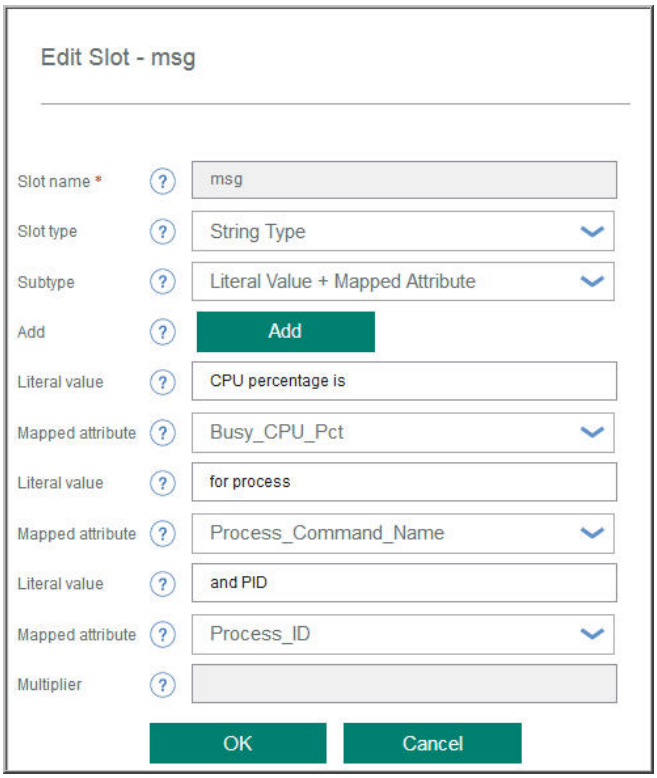
Después de pulsar **Aceptar** para cerrar la ventana, la ventana **Personalización de atributo EIF** listará el nombre de atributo y si está personalizado.

6. Cuando termine de editar el atributo base EIF o de añadir, suprimir o editar atributos personalizados EIF para el umbral, pulse **Aceptar**.
7. Cuando haya terminado de editar el umbral, pulse **Guardar**.

   Para obtener más información, consulte “Gestor de umbrales” en la página 1019.

Ejemplo

El umbral `Linux_BP_ProcHighCpu_Critical` comprueba si el consumo de CPU es del 95% o superior. Para añadir el porcentaje de CPU ocupada, el nombre de mandato de proceso y el ID de proceso al mensaje de resumen (incluido en el atributo msg), el atributo msg se ha personalizado con tres conjuntos de campos de **Valor literal** y **Atributo correlacionado**:



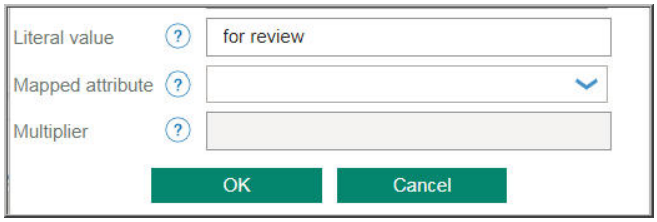
La plantilla de mensaje tiene el aspecto siguiente:

```
El porcentaje de CPU es Por_CPU_ocupada para el proceso nommbre_mandato_proceso y el PID
ID_proceso
```

Y el mensaje resultante que se visualiza en el Gestor de sucesos podría se similar al siguiente:

`El porcentaje de CPU es 97 para el proceso large.exe y el PID 9876`

También puede añadir los campos **Valor literal** y **Atributo correlacionado** y dejar un campo vacío. Por ejemplo, para añadir "para revisar" a la plantilla de mensaje, pulse **Añadir** y especifique `para revisar` para **Valor literal**.



Ahora la plantilla de mensaje tiene el siguiente aspecto:

`El porcentaje de CPU es Por_CPU_ocupada para el proceso nombre_mandato_proceso y el PID ID_proceso para revisar`

Y el mensaje resultante que se visualiza en el **Gestor de sucesos** podría ser similar al siguiente:

`El porcentaje de CPU es 96 para el proceso big.exe y el PID 5432 para revisar`

Qué hacer a continuación

Si ha creado nuevos atributos personalizados de EIF, debe identificar los atributos nuevos en la tabla de `alerts.status` de su Netcool/OMNIbus ObjectServer, a continuación actualice el archivo de configuración `itm_apm_event.rules` instalado durante la integración de Netcool/OMNIbus con Cloud APM.

Adición de atributos personalizados de EIF a la base de datos de Netcool/OMNIbus ObjectServer

Cuando añade atributos personalizados de EIF nuevos para umbrales, debe identificarlos en su receptor de EIF para poder ver sucesos reenviados que utilizan los atributos personalizados. Si tiene Netcool/OMNIbus integrado con Cloud APM, actualice la tabla `alerts.status` para definir los atributos nuevos.

Acerca de esta tarea

Cuando configuró la integración de Netcool/OMNIbus con Cloud APM, en el paso “4” en la página 1003 tuvo que cargar `itm_apm_db_update.sql`. El procedimiento siguiente está destinado a utilizar la interfaz SQL interactiva para actualizar la tabla `alerts.status` en la base de datos de `itm_apm_db_update.sql`.

Procedimiento

Siga estos pasos en Netcool/OMNIbus ObjectServer para definir los atributos personalizados de EIF nuevos creados en el **Editor de umbrales**:

1. Inicie la interfaz interactiva de SQL para editar la base de datos:

   Linux

   ```
   $OMNIHOME/bin/nco_sql -user nombre_usuario -password contraseña
   -server
   nombre_servidor > itm_apm_db_update.sql
   ```

   Ejemplo:

   ```
   $OMNIHOME/bin/nco_sql -user smadmin -password passw0rd -server NCOMS >
   /tmp/apm/itm_apm_db_update.sql
   ```

   Windows

   ```
   itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U nombre_usuario
   -P contraseña -S nombre_servidor
   ```

   Ejemplo:

```
\temp\apm\itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U smadmin
-P passw0rd -S NCOMS
```

2. Para cada atributo personalizado de EIF, especifique el mandato SQL **ALTER TABLE** con el nombre de atributo personalizado y el tipo de atributo en el formato siguiente, pulse Intro y, a continuación, especifique go y pulse Intro:
   - Para un tipo de atributo de serie, teclee

     ```
     alter table alerts.status add NombreAtributoPersonalizado varchar(512);
     ```

   - Para un tipo de atributo de número, teclee

     ```
     alter table alerts.status add NombreAtributoPersonalizado integer;
     ```

   donde *NombreAtributoPersonalizado* es el nombre del atributo personalizado de EIF exactamente como se especificó en el campo **Nombre de atributo** de la ventana **Añadir atributo** del **Editor de umbrales**.

Ejemplo

El ejemplo muestra los mandatos **alter table** para añadir los atributos personalizados **BusinessApplication** y **GenericMetric**.

```
alter table alerts.status add BusinessApplication varchar(512);
```

```
alter table alerts.status add GenericMetric integer;
```

Qué hacer a continuación

Actualice el archivo de configuración `itm_apm_event.rules` instalado como parte de la integración de Netcool/OMNIbus con Cloud APM. Para obtener más información, consulte “Adición de atributos personalizados de EIF a reglas de sucesos de receptor de EIF” en la página 1029.

Adición de atributos personalizados de EIF a reglas de sucesos de receptor de EIF

Si ha definido atributos personalizados de EIF nuevos para umbrales, debe actualizar el archivo de reglas para identificar los atributos nuevos para el receptor de EIF.

Acerca de esta tarea

Estos pasos le permiten actualiza el archivo `itm_apm_event.rules` en Netcool/OMNIbus Probe for Tivoli EIF para identificar cada atributo personalizado de EIF nuevo. Si está utilizando otro receptor de EIF, actualice los archivos de reglas según sea necesario para el receptor.

Procedimiento

1. En el sistema en el que Probe for Tivoli EIF está instalado, vaya al directorio de instalación

   Linux cd *dir_instalación*`/tivoli/netcool/omnibus/probes/linux2x86`

   Windows cd *dir_instalación*`\Tivoli\Netcool\omnibus\probes\win32`

   donde *dir_instalación* es el valor predeterminado `/opt/IBM/` o `C:\IBM\` o el directorio especificado cuando se instaló el análisis.
2. Haga una copia de seguridad del archivo `itm_apm_event.rules`.
3. Abra el archivo Probe for Tivoli EIF `itm_apm_event.rules` en un editor de texto.

   El archivo tiene tres partes que está editando para añadir el atributo de EIF personalizado (o los atributos) creados.
4. Añada las sentencias **if** con una sentencia nueva para cada atributo de EIF que utiliza el formato siguiente:

```
    if(exists($NombreAtributoPersonalizado))
    {
        if(regmatch($NombreAtributoPersonalizado, "^'.*'$"))
        {
            $SourceType = extract($NombreAtributoPersonalizado, "^'(.*)'$")
        }
    }
```

donde *NombreAtributoPersonalizado* es el nombre del atributo personalizado de EIF exactamente como se especificó en el campo **Nombre de atributo** de la ventana **Añadir atributo**.

5. Añada la lista de entradas de `@` con una fila nueva para cada atributo personalizado de EIF que utiliza el formato siguiente:

```
@NombreAtributoPersonalizado=$NombreAtributoPersonalizado
```

donde *NombreAtributoPersonalizado* es el nombre del atributo personalizado de EIF.

6. Añada la lista de entradas de `$tmpEventData` con una fila nueva para cada atributo personalizado de EIF que utiliza el formato siguiente:

```
$tmpEventData = nvp_remove( $tmpEventData, "NombreAtributoPersonalizado")
```

donde *NombreAtributoPersonalizado* es el nombre del atributo personalizado de EIF.

7. Guarde y cierre el archivo `itm_apm_event.rules`.
8. Reinicie Probe for Tivoli EIF para implementar sus actualizaciones.

Resultados

Este archivo de reglas está actualizado y Probe for Tivoli EIF puede procesar ahora sucesos de umbral que utilizan las los atributos personalizados de EIF nuevos y reenvían los detalles de suceso al Netcool/OMNIbus ObjectServer.

Ejemplo

A continuación se proporciona un extracto de `itm_apm_event.rules` después de editarlo para añadir estos atributos personalizados de EIF: **BusinessApplication** y **GenericMetric** (mostrados en cursiva).

```
# ------------------------------------------------------------
    if(exists($SourceID))
    {
        if(regmatch($SourceID, "^'.*'$"))
        {
            $SourceID = extract($SourceID, "^'(.*)'$")
        }
    }
    ...
    ...
    ...
    if(exists($ManagedSystemGroups))
    {
        if(regmatch($ManagedSystemGroups, "^'.*'$"))
        {
            $SourceType = extract($ManagedSystemGroups, "^'(.*)'$")
        }
    }
    if(exists($BusinessApplication))
    {
        if(regmatch($BusinessApplication, "^'.*'$"))
        {
            $SourceType = extract($BusinessApplication, "^'(.*)'$")
        }
    }
     if(exists($GenericMetric))
    {
        if(regmatch($GenericMetric, "^'.*'$"))
        {
            $SourceType = extract($GenericMetric, "^'(.*)'$")
        }
    }
```

```
@SourceID=$SourceID
@URL=$ManagementURL
@Service=$Service
@SourceType=$SourceType
@SubscriberID=$TenantID
@APMHostname=$apm_hostname
@ManagedSystemGroups=$ManagedSystemGroups
@BusinessApplication=$BusinessApplication
@GenericMetric=$GenericMetric

# ------------------------------------------------------------------
# -  RTC 66157
# ------------------------------------------------------------------
if ( exists ( $appl_label ) )
{
   if ( match($appl_label, "PI:A:S"))
   {
       @Class = 87723
   }
}
# ------------------------------------------------------------------
# -  RTC 48775 - APM FP5 agents do not populate data in email of EMaaS Basic
# ------------------------------------------------------------------
if (match( $situation_eventdata, "~" ) )
{
   # Dump all fields into the ITMEventData field
   $tmpEventData = nvp_add($*)
   # Remove the duplicated fields
   $tmpEventData = nvp_remove( $tmpEventData, "appl_label")
   $tmpEventData = nvp_remove( $tmpEventData, "control")
   ...
   ...
   ...
   $tmpEventData = nvp_remove( $tmpEventData, "ManagedSystemGroups")
   $tmpEventData = nvp_remove( $tmpEventData, "EventSeqNo")
   $tmpEventData = nvp_remove( $tmpEventData, "BusinessApplication")
   $tmpEventData = nvp_remove( $tmpEventData, "GenericMetric")
      @ITMEventData = $tmpEventData
```

Enviar un correo electrónico en respuesta a un suceso

Solo Cuando su entorno gestionado incluye IBM Alert Notification, puede proporcionar una notificación por correo electrónico cuando el rendimiento de la aplicación supere los umbrales.

Acerca de esta tarea

Para configurar la notificación de correo electrónico, debe habilitar IBM Alert Notification tal como se describe en Recopilación de temas de notificación de alertas en IBM Knowledge Center. A continuación, añada las aplicaciones supervisadas a los grupos de recursos. Para cada grupo de recursos, puede configurar una o varias direcciones de correo electrónico. Cuando el rendimiento de una aplicación de un grupo sobrepasa un umbral, se recibe una notificación de correo electrónico en las direcciones configuradas para el grupo.

Procedimiento

1. Pulse **Configuración del sistema** > **Gestor de grupos de recursos**.
2. Pulse **Nuevo** para crear el grupo de recursos para el que desee configurar la notificación de correo electrónico o seleccione un grupo existente y pulse **Editar**.

   Se abre el **Editor de grupo de recursos**.
3. pulse **Configurar notificación de correo electrónico** para abrir la aplicación IBM Alert Notification en una pestaña o una ventana de navegador nueva. Utilice Alert Notification para crear usuarios y asociar las direcciones de correo electrónico a los grupos de recursos para recibir notificaciones de sucesos por correo electrónico.

Utilización de la API Servicio de gestión de grupos de recursos

Utilice la API Servicio de gestión de grupos de recursos para gestionar el ciclo de vida de grupos de sistemas gestionados desde la línea de mandatos.

Acerca de esta tarea

Realice tareas de grupos de recursos como crear, ver, actualizar y suprimir grupos de sistemas gestionados. Añada y elimine sistemas individuales de grupos personalizados. Visualice una lista de sistemas que ha añadido a un grupo específico de recursos personalizados y visualice una lista de sistemas que se añaden automáticamente a los grupos incorporados, como el grupo de recursos del sistema.

Puede crear scripts para automatizar tareas como la definición de grupos de recursos y la asignación de agentes a estos grupos de recursos. Los grupos de recursos pueden ser destinos de distribuciones de umbrales y/o políticas de control de accesos.

Las operaciones siguientes se describen en API Explorer y en el ejemplo que figura al final de este tema.

- Devolver todos los grupos de recursos, agentes o un agente o grupo de recursos específico
- Crear un grupo de recursos personalizado o actualizar la definición de un grupo existente
- Suprimir un grupo de recursos personalizado especificado
- Añadir agentes a un grupo de recursos personalizado
- Eliminar agentes de un grupo de recursos personalizado

Procedimiento

Complete estos pasos para definir y modificar grupos de recursos personalizados con la API Servicio de gestión de grupos de recursos. Los agentes y grupos de recursos del sistema no se pueden modificar.

1. Complete del paso 1 al paso 9 del tema Exploración de las API.
   El paso 10 y el paso 11 proporcionan detalles adicionales.
2. Pulse **USE** y seleccione una clave, por ejemplo, **Key1**.

   Nota: Pulse **Ocultar** para mostrar el ID de cliente y el secreto de cliente. Anótelos porque, si está realizando llamadas de API con herramientas externas fuera del Explorador de API, son necesarios. A continuación, pulse **Mostrar** para ocultarlos.
3. Complete todas las cabeceras necesarias, indicadas con un asterisco.

   X-IBM-Service-Location
   * la cabecera es la ubicación geográfica de la suscripción, como por ejemplo na para Norteamérica

   Autorización
   * la cabecera es la serie codificada en base64 del ID y contraseña de IBM. Al codificar el ID y contraseña de IBM en la herramienta de codificación en based64, el formato debe ser *idIBM:contraseña*, por ejemplo, `Basic YXBtYWRtaW46YXBtcGFzcw==!`.
4. Debe incluir una cabecera de referenciador en todas las solicitudes POST, PUT y DELETE. El valor de la cabecera Referer es siempre:

   ```
   -H 'Referer: https://api.ibm.com'
   ```
5. Desplácese hasta localizar y pulse **Probar**.

Resultados

Los cambios que realice en los grupos de recursos personalizados en la API entran en vigor de inmediato y se visualizan en el **Gestor de grupo de recursos** (consulte “Gestor de grupos de recursos” en la página 1014).

Ejemplo

Este mandato devuelve los nombres, identificadores exclusivos, estado, nombre de host, versión, y el tipo de agente para todos los agentes:

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes=Agent&_field=keyIndexName&
_field=online&_field=hostname&_field=version&_field=productCode&_field=description
```

Este mandato devuelve una lista de todos los agentes de sistema operativo Linux:

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes=Agent&_filter=description=
"Linux OS"&_field=keyIndexName
```

Este mandato devuelve una lista de grupos personalizados y del sistema:

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes:AgentGroup,
AgentSystemGroup&_field=keyIndexName&_field=displayLabel
```

Este mandato devuelve la lista de agentes que se han asignado a un grupo que tiene el identificador exclusivo {id}:

```
GET /1.0/topology/mgmt_artifacts/{id}/references/to/contains
```

El ejemplo siguiente utiliza el mandato curl para crear un grupo personalizado.

```
POST /1.0/topology/mgmt_artifacts
```

Nota: El cuerpo de la solicitud POST debe contener un objeto JSON que define el grupo según lo mostrado por el parámetro **-d**.

```
curl -X POST \
  https://api.ibm.com/perfmgmt/run/1.0/topology/mgmt_artifacts \
  -H 'Referer: https://api.ibm.com' \
  -H 'authorization: Basic REPLACE_BASE64_ENCODED_STRING' \
  -H 'content-type: application/json' \
  -H 'x-ibm-client-id: REPLACE_KEY_VALUE' \
  -H 'x-ibm-client-secret: REPLACE_KEY_VALUE' \
  -d '{
  "keyIndexName": "customGroup",
  "description": "Descripción de grupo personalizado",
  "displayLabel": "customGroupLabel",
  "entityTypes": [
    "AgentGroup"
  ],
  "arbitraryStringProperty": "Su valor de propiedad personalizada"
}'
```

Este mandato añade un agente con identificador exclusivo {otherid} a un grupo personalizado que tiene identificador exclusivo {id}:

```
POST /1.0/topology/mgmt_artifacts/{id}/references/to/contains/{otherid}
```

Este mandato elimina un agente con identificador exclusivo {otherid} de un grupo personalizado que tiene identificador exclusivo {id}:

```
DELETE /1.0/topology/mgmt_artifacts/{id}/references/to/contains/{otherid}
```

Utilización de la API del servicio de gestión de umbrales

Utilice la API Servicio de gestión de umbrales para gestionar el ciclo de vida de los umbrales de supervisión desde la línea de mandatos.

Acerca de esta tarea

Realice tareas de gestor de umbrales como crear, ver, actualizar y suprimir umbrales. Asigne grupos de recursos a estos umbrales. Visualice una lista de todas las asignaciones de umbrales y recursos. Visualice una lista de todos los umbrales que están asignados a un grupo de recursos específico.

Puede crear scripts para automatizar tareas como la definición de umbrales y la asignación de estos umbrales a grupos de recursos.

Las operaciones siguientes se describen en API Explorer y en el ejemplo que figura al final de este tema.

- Devolver todos los umbrales u obtener un umbral específico. Puede filtrar la solicitud con estos atributos: **label**, que corresponde al nombre del umbral; **_appliesToAgentType**, que corresponde al código de producto de dos caracteres y **_uiThresholdType**, que corresponde al tipo de umbral que

se muestra en las páginas del editor Gestor de umbrales y Grupo de recursos de la Consola de Cloud APM. Puede utilizar **_offset** o **_limit** al obtener umbrales

- Crear un umbral o actualizar la definición de un umbral existente Debe incluir la cabecera X-HTTP-Method-Override y establecerla en PATCH para la solicitud de actualización
- Suprimir un umbral especificado
- Devolver todas las asignaciones de recursos o una asignación de recursos específica, que muestre los umbrales que están asignados a cada grupo de recursos. Puede filtrar la solicitud con estos atributos: **resource._id** y **threshold._id**; y utilizar estos operadores soportados **=** (igual) y **!=** (no igual)
- Crear una asignación de recursos, que asigne un solo umbral a un solo grupo de recursos
- Suprimir una asignación de recursos, que elimina un único umbral de un único grupo de recursos

Procedimiento

1. Complete del paso 1 al paso 9 del tema Exploración de las API.
   El paso 10 y el paso 11 proporcionan detalles adicionales.
2. Pulse **USE** y seleccione una clave, por ejemplo, **Key1**.

   Nota: Pulse **Ocultar** para mostrar el ID de cliente y el secreto de cliente. Anótelos porque, si está realizando llamadas de API con herramientas externas fuera del Explorador de API, son necesarios. A continuación, pulse **Mostrar** para ocultarlos.
3. Complete todas las cabeceras necesarias, indicadas con un asterisco.

   X-IBM-Service-Location
   * la cabecera es la ubicación geográfica del servidor, como por ejemplo na para Norteamérica

   Authorization
   * la cabecera es la serie codificada en base 64 del IBMid y la contraseña. Al codificar el IBMid y la contraseña en la herramienta de codificación en based64, el formato debe ser *idIBM:contraseña*. Por ejemplo, `Basic YXBtYWRtaW46YXBtcGFzcw==!`.
4. Desplácese hasta localizar y pulse **Probar**.

Ejemplo

Este mandato devuelve todos los umbrales registrados con el servidor:

```
GET /threshold_types/itm_private_situation/thresholds
```

Este mandato devuelve la información del umbral con la etiqueta (nombre) `My_threshold`.

```
GET /threshold_types/itm_private_situation/thresholds?_filter=label%3DMy_threshold
```

Este mandato devuelve todos los umbrales para el tipo de agente LZ, que es el código de componente para el Agente de sistema operativo Linux.

```
GET /threshold_types/itm_private_situation/thresholds?_filter=_appliesToAgentType%3DLZ
```

Este mandato tiene la misma salida que el mandato anterior pero se da el nombre de agente tal como aparece en la Consola de Cloud APM.

```
GET /threshold_types/itm_private_situation/thresholds?_filter=_uiThresholdType%3DLinux OS
```

Este mandato devuelve todos los grupos de recursos a los que está asignado el umbral 123:

```
GET /resource_assignments?_filter=threshold._id=123
```

El ejemplo siguiente utiliza el mandato curl para crear un umbral.

```
POST /1.0/thresholdmgmt/threshold_types/itm_private_situation/thresholds
```

Recuerde: El cuerpo de la solicitud POST debe contener un objeto JSON que defina el umbral según lo mostrado por el parámetro **-d**.Ejemplo:

```
curl -X POST\
 https://api.ibm.com/perfmgmt/run/1.0/thresholdmgmt/threshold_types/itm_private_situation/
thresholds  \
  -H 'authorization: Basic REPLACE_BASE64_ENCODED_STRING' \
  -H 'content-type: application/json' \
  -H 'x-ibm-client-id: REPLACE_KEY_VALUE' \
  -H 'x-ibm-client-secret: REPLACE_KEY_VALUE' \
  -d '{
  "label": "Your_Linux_Threshold_Name",
  "description": "Your Linux Threshold Definition",
  "configuration": {
    "type": "json",
    "payload": {
      "formulaElements": [
        {
          "function": "*MKTIME",
          "metricName": "KLZ_CPU.Timestamp",
          "operator": "*EQ",
          "threshold": "1455767100000",
          "timeDelta": {
            "operator": "+",
            "delta": "3",
            "unit": "Hours"
          }
        }
      ],
      "period": "011500",
      "periods": "3",
      "severity": "Fatal",
      "matchBy": "KLZCPU.CPUID",
      "operator": "*OR",
      "actions": [
        {
          "name": "command",
          "command": "ps -ef",
          "commandFrequency": "Y",
          "commandWhen": "Y",
          "commandWhere": "N"
        }
      ]
    }
  }
}'
```

Gestión del acceso de usuarios

Utilice las características de Control de accesos basado en roles de Cloud APM para otorgar a los usuarios los privilegios de acceso que necesitan para su rol.

La seguridad de Cloud APM está basada en roles. Un rol es un grupo de permisos que controla las acciones que puede realizar en Cloud APM. Puede crear roles personalizados en Cloud APM. Puede asignar permisos a roles personalizados o puede asignar más permisos a roles predeterminados existentes. Puede asignar usuarios y grupos de usuarios a roles predeterminados existentes o a roles personalizados. Puede asignar usuarios y grupos de usuarios a varios roles. Los permisos son acumulativos, a un usuario o a un grupo de usuarios se le asignan todos los permisos correspondientes a todos los roles a los que están asignados.

La autenticación de usuario en Cloud APM se gestiona a través de IBM Marketplace, o se puede gestionar a través de Collaborative Operations, si tiene una suscripción.

La autenticación de usuario en Performance Management requiere un id de IBM. Cree un IBMid seleccionando el enlace **Crear un IBMid** en la página **Iniciar sesión en IBM**. Para acceder a la página **Iniciar sesión en IBM**, vaya a la página **Productos y servicios** (http://ibm.biz/my-prodsvcs) en IBM Marketplace y se le redigirá a la página **Iniciar sesión en IBM** (es posible que tenga que cerrar sesión y volver a la página **Productos y servicios** (http://ibm.biz/my-prodsvcs)).

Una vez que tenga un IBMid, puede iniciar sesión en Cloud APM, directamente o desde Productos y servicios. La autorización para acceder a una instancia de Cloud APM se gestiona a través de **Productos y servicios** o a través de Collaborative Operations, si tiene una suscripción. De forma predeterminada, el usuario que solicita una prueba o adquiere una suscripción tiene privilegios de administrador.

El propietario de la suscripción de Cloud APM es el usuario predeterminado en Cloud APM. Es el usuario que solicita una prueba o adquiere una suscripción. Este usuario predeterminado es miembro del rol Administrador de roles y tiene privilegios de administrador que le permite añadir nuevos usuarios. Los usuarios subsiguientes se añaden de forma predeterminada al rol Usuario de supervisión.

Si no es miembro de un rol e intenta iniciar una sesión en Cloud APM, recibirá un mensaje **No autorizado**.

Para añadir un usuario de Cloud APM:

1. Vaya a **Productos y servicios** en IBM Marketplace y expanda el widget **IBM Performance Management**.
2. Pulse **Gestionar autorizaciones** y entre un ID de IBM o una dirección de correo electrónico en los campos **Añadir nuevo usuario** o **Buscar usuarios existentes**. Pulse **Añadir usuario** para añadir el usuario.

No hay límite en el número de usuarios que puede añadir a una suscripción de Cloud APM.

Nota: El soporte no se ofrece para grupos de usuarios en Cloud APM.

Para obtener más información sobre los roles, consulte "Roles y permisos" en la página 1036.

Roles y permisos

Un *rol* es un grupo de permisos que controlan las acciones que puede realizar en Cloud APM. Utilice la página Control de accesos basado en roles para gestionar usuarios y roles o, de forma alternativa, utilice la API de autorización para completar tareas de control de accesos basado en roles desde la línea de mandatos. Para obtener más información, consulte "Exploración de las API" en la página 1107.

Cloud APM tiene cuatro roles predeterminados:

Administrador de roles
Este rol está pensado para los usuarios cuya función de trabajo principal es crear políticas de control de acceso para Cloud APM. Este rol tiene todos los permisos. Si cambia el usuario predeterminado, el usuario predeterminado nuevo se convierte automáticamente en un miembro del Administrador de roles. Este rol no se puede editar. Los administradores de roles no pueden eliminarse a sí mismos del rol Administrador de roles. Esta restricción elimina el riesgo de eliminar accidentalmente todos los usuarios del rol Administrador de roles.

Administrador de supervisión
Este rol está pensado para los usuarios cuya función de trabajo principal es utilizar Cloud APM para supervisar los sistemas. Los administradores de supervisión realizan tareas como por ejemplo añadir aplicaciones de supervisión, crear umbrales, añadir grupos de recursos y distribuir los umbrales a esos grupos de recursos. Este rol se puede editar.

Administrador del sistema
Este rol está pensado para los usuarios cuya función de trabajo primaria sea realizar tareas de administración para el sistema Cloud APM. Los administradores del sistema realizan tareas como por ejemplo configurar el Gestor de sucesos o configurar la Pasarela híbrida. Este rol se puede editar.

Usuario de supervisión
Este rol está pensado para los usuarios cuya función de trabajo primaria es configurar y mantener el buen estado de los sistemas supervisados por Cloud APM.Este rol se puede editar.

En la tabla siguiente se describen los permisos que puede asignar a los roles, así como los cuatro roles predeterminados disponibles y sus permisos asociados:

Tabla 237. Roles y permisos								
	Administrador de roles		**Administrador de supervisión**		**Administrador del sistema**		**Usuario de supervisión**	
	Ver	**Modificar**	**Ver**	**Modificar**	**Ver**	**Modificar**	**Ver**	**Modificar**
Permisos de configuración del sistema								
Configuración avanzada	✓	N/A	—	N/A	✓	N/A	—	N/A
Configuración del agente	✓	N/A	✓	N/A	—	N/A	—	N/A
Páginas informativas	✓	N/A	✓	N/A	✓	N/A	✓	N/A
Proveedor de búsqueda	✓	N/A	✓	N/A	—	N/A	—	N/A
Estadísticas de uso	✓	N/A	✓	N/A	—	N/A	—	N/A
Permisos de recursos								
Panel de instrumentos del rendimiento de aplicaciones	✓	✓	✓	✓	✓	—	✓	—
Aplicaciones	✓	✓	✓	✓	—	—	✓	—
Aplicación individual	“Permisos de aplicación y grupo de recursos” en la página 1041							
Panel de instrumentos de diagnóstico	✓	N/A	—	N/A	—	N/A	—	N/A
Gestor de grupos de recursos	✓	N/A	✓	N/A	—	N/A	—	N/A
Grupo de recursos individual	“Permisos de aplicación y grupo de recursos” en la página 1041							
Grupos de recursos	✓	✓	✓	✓	—	—	—	—
Gestor de scripts sintéticos	✓	N/A	—	N/A	—	N/A	—	N/A
Gestor de umbrales	✓	N/A	✓	N/A	—	N/A	—	N/A

Donde

✓ indica que los miembros de este rol tienen este permiso

— indica que los miembros de este rol no tienen este permiso

N/A indica que este permiso no existe

Nota: Aunque **Estadísticas de uso** se visualiza en la lista de **Permisos de configuración del sistema**, ya no es aplicable a Cloud APM.

La tabla siguiente describe las acciones asociadas a cada permiso:

Tabla 238. Permisos	
Permiso	**Descripción**
Configuración avanzada	Si tiene permiso para ver, puede realizar las siguientes tareas: • Ver **Configuración del sistema** > **Configuración avanzada** en la barra de menús. • Realizar y guardar cambios en la ventana **Configuración avanzada**. • Ver **Configuración del sistema** > **Hybrid Gateway Manager** en la barra de menús. • Realizar y guardar cambios en la ventana **Hybrid Gateway Manager**.

Tabla 238. Permisos (continuación)	
Permiso	**Descripción**
Configuración del agente	Si tiene permiso para ver, puede realizar las siguientes tareas: • Ver **Configuración del sistema** > **Configuración del agente** en la barra de menús. • Realizar y guardar cambios en la ventana **Configuración del agente**.
Páginas informativas	Si tiene permiso para ver, puede realizar la siguiente tarea: • Ver **Cómo empezar** y **Ayuda** en la barra de menús. **Nota:** Cuando se abre la página **Cómo empezar**, si desactiva **Mostrar esta página en el inicio**, para inicios de sesión posteriores, verá un error de permiso rechazado. Sin embargo, aún podrá navegar a la página **Cómo empezar** y a las otras áreas para las que tenga permiso.
Proveedor de búsqueda	Si tiene permiso para ver, puede realizar las siguientes tareas: • Ver **Configuración del sistema** > **Configurar proveedores de búsqueda** en la barra de menús. • Realizar y guardar cambios en la página **Configurar proveedores de búsqueda**.

Tabla 238. Permisos (continuación)

Permiso	Descripción
Panel de instrumentos del rendimiento de aplicaciones	Si tiene permiso para ver, puede realizar las siguientes tareas: • Ver **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** en la barra de menús. • Ver el Panel de instrumentos del rendimiento de aplicaciones y las aplicaciones predefinidas **Mis componentes** y **Mis transacciones**. **Nota:** Para determinar qué permisos son necesarios para ver los sistemas en la aplicación Mis componentes, consulte "Permisos de aplicación y grupo de recursos" en la página 1041. **Nota:** La aplicación Mis transacciones solo se visualiza si está utilizando la supervisión del sitio web. Todas las transacciones sintéticas de supervisión de sitio web se visualizan en la aplicación Mis transacciones. • Abrir páginas personalizadas del panel de instrumentos en la pestaña Vistas personalizadas. • Crear vistas en la pestaña Detalles de atributo y guardarlas para su propio uso. Si tiene permiso para modificar, puede realizar las siguientes tareas: • Ver **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** en la barra de menús. • Ver el Panel de instrumentos del rendimiento de aplicaciones y las aplicaciones predefinidas **Mis componentes** y **Mis transacciones**. **Nota:** Para determinar qué permisos son necesarios para ver los sistemas en la aplicación Mis componentes, consulte "Permisos de aplicación y grupo de recursos" en la página 1041. **Nota:** La aplicación Mis transacciones solo se visualiza si está utilizando la supervisión del sitio web. Todas las transacciones sintéticas de supervisión de sitio web se visualizan en la aplicación Mis transacciones. • Crear y guardar páginas personalizadas del panel de instrumentos en la pestaña Vistas personalizadas. • Crear vistas en la pestaña Detalles de atributo y compartirlas con otros. • Visualizar la opción **Acciones**>**Editar** en las páginas de componente. Esta opción le permite editar los valores de umbral y otros valores de los widget de grupo que se visualizan en el panel de instrumentos Componentes.
Aplicaciones	Si tiene permiso para ver, puede realizar las siguientes tareas: • Ver aplicaciones en Panel de instrumentos de aplicaciones. Si tiene permiso para modificar, puede realizar las siguientes tareas: • Ver aplicaciones en Panel de instrumentos de aplicaciones • Crear, modificar y suprimir aplicaciones con las herramientas en Panel de instrumentos de aplicaciones.
Aplicación individual	Consulte "Permisos de aplicación y grupo de recursos" en la página 1041.
Gestor de grupos de recursos	Si tiene permiso para ver, puede realizar la siguiente tarea: • Ver **Configuración del sistema** > **Gestor de grupos de recursos** en la barra de menús.

Tabla 238. Permisos (continuación)	
Permiso	**Descripción**
Grupos de recursos	Si tiene permiso para ver, puede realizar las siguientes tareas: • Ver grupos de recursos y los sistemas en ellos en el Gestor de grupos de recursos si también tiene el permiso de visualización del Gestor de grupos de recursos. • Ver los sistemas en la aplicación predefinida Mis componentes si también tiene el permiso de modificación o el permiso de visualización de Application Performance Management. • Ver los sistemas en la ventana **Añadir aplicación** si también tiene permiso para modificar aplicaciones. Si tiene permiso para modificar, puede realizar las siguientes tareas: • Ver grupos de recursos y sus contenidos en el Gestor de grupos de recursos si también tiene permiso de visualización de Gestor de grupos de recursos. • Ver los sistemas en la aplicación predefinida Mis componentes si también tiene permiso de visualización o modificación de Application Performance Management. • Ver los sistemas en la ventana **Añadir aplicación** si también tiene permiso para modificar aplicaciones. • Crear, modificar y suprimir grupos de recursos en el Gestor de grupos de recursos si también tiene permiso de visualización de Gestor de grupos de recursos. Para asignar umbrales a un grupos de recursos, necesita también ser miembro de un rol que tenga permiso de visualización para el Gestor de umbrales. **Nota:** El Gestor de grupos de recursos se utiliza para organizar sistemas supervisados en grupos, de modo que se puedan asignar umbrales a estos grupos. Si no tiene permiso de visualización para el Gestor de umbrales, no podrá ver los umbrales asignados a grupos de recursos. Si asigna conjuntamente el permiso de modificación de grupos de recursos a un rol, también es necesario asignar al rol el permiso de visualización de gestor de umbrales.
Grupos de recursos individual	Consulte “Permisos de aplicación y grupo de recursos” en la página 1041.
Gestor de umbrales	Si tiene permiso para ver, puede realizar las siguientes tareas: • Ver **Configuración del sistema** > **Gestor de umbrales** en la barra de menús. • Crear, modificar y suprimir umbrales en el Gestor de umbrales. • Ver y editar la asignación de grupos de recursos para umbrales en el Gestor de umbrales si tiene los permisos adecuados para el grupo o los grupos de recursos. • Como alternativa, ver y editar la asignación de umbrales para los grupos de recursos en el Gestor de grupos de recursos si tiene los permisos adecuados para el Gestor de grupos de recursos y el grupo o los grupos de recursos, y permiso de visualización para el Gestor de umbrales.

Tabla 238. Permisos (continuación)	
Permiso	**Descripción**
Gestor de scripts sintéticos	Si tiene permiso para ver, puede realizar las siguientes tareas: • Crear, modificar y suprimir transacciones sintéticas en el Gestor de transacciones sintéticas. **Nota:** Para trabajar con transacciones sintéticas en el Gestor de transacciones sintéticas, también es necesario ser miembro de un rol que tenga permiso para ver para la **Configuración de agente**.
Panel de instrumentos de diagnóstico	Si tiene permiso de visualización, el botón **Diagnostica** está habilitado en los paneles de instrumentos de diagnóstico para Agente de WebSphere Applications, Agente de Node.js, Agente de Ruby y Agente de Microsoft .NET. Pulse el botón **Diagnosticar** para profundizar en los paneles de instrumentos de diagnóstico.

Permisos de aplicación y grupo de recursos
Los permisos se pueden asignar a aplicaciones individuales y grupos de recursos.

Permisos de aplicación

En Cloud APM, una aplicación es un grupo de componentes y las instancias dentro de estos componentes. Utilice la ventana **Añadir aplicación** para definir una aplicación. Si desea más información sobre cómo definir una aplicación, consulte Gestión de aplicaciones.

Para seleccionar **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** en la Consola de Cloud APM, debe tener asignado el permiso de visualización y modificación para el Panel de instrumentos del rendimiento de aplicaciones. Este permiso también le permite ver las aplicaciones predefinidas **Mis componentes** y **Mis transacciones**. La aplicación **Mis transacciones** se visualiza solo si está utilizando la supervisión del sitio web. Para ver otras aplicaciones personalizadas, debe tener permiso de visualización o permiso de modificación para todas las aplicaciones o para una aplicación individual.

Nota: Si se renombra una aplicación, los permisos no se retienen; deben volver a asignar permisos de visualización y modificación.

Ver

El permiso de visualización en una aplicación tiene prioridad sobre cualquier otro permiso. Para ver una aplicación, no es necesario ser miembro de un rol que tenga permiso de visualización para cada componente e instancia de componente de la aplicación. La tabla siguiente describe las acciones que puede realizar si tiene permiso de visualización para una aplicación:

Tabla 239. Ver permiso para una aplicación	
Acción	**Permiso disponible**
Ver todos los componentes de soporte de dicha aplicación.	✓
Ver la aplicación y sus componentes en el árbol de navegación.	✓
Ver los componentes de aplicación en Mis componentes.	✓
Ver páginas de panel de instrumentos personalizadas asociadas con la aplicación.	✓
Agregar o eliminar componentes de la aplicación.	—

Tabla 239. Ver permiso para una aplicación (continuación)	
Acción	**Permiso disponible**
Asignar umbrales a los componentes de las aplicaciones.	—
Ver los componentes de soporte de una aplicación en el Gestor de grupos de recursos.	—

Modificar

Si es miembro de un rol que tiene permiso de modificación en una aplicación individual, puede

- Suprimir la aplicación.
- Crear páginas personalizadas del panel de instrumentos en la pestaña Vistas personalizadas. Consulte "Vistas personalizadas" en la página 1147.
- Agregar o eliminar componentes e instancias de componente mediante la ventana **Editar aplicación**. Los componentes e instancias de componente que están disponibles en la ventana **Editar aplicación** se filtran según los permisos de rol que tenga. Están disponibles los componentes siguientes:
  - Los componentes para los que tiene permiso de acceso directamente en los grupos de recursos del sistema y en el grupo de recursos personalizados
  - Los componentes de los que ha heredado indirectamente los permisos basándose en otras aplicaciones para las que tiene permiso de modificación

Permisos de grupo de recursos

Utilice Grupos de recursos para agrupar componentes por su tipo o finalidad. Si desea más información sobre cómo crear grupos de recursos, consulte "Gestor de grupos de recursos" en la página 1014.

Para seleccionar **Configuración del sistema** > **Gestor de grupos de recursos**, debe tener asignado el permiso de visualización del Gestor de grupos de recursos. Para ver grupos de recursos en el **Gestor de grupos de recursos** o para ver miembros de grupos de recursos en la aplicación **Mis componentes**, también debe tener asignado el permiso de visualización o modificación para todos los grupos de recursos o para los grupos de recursos individuales.

Existen dos tipos de grupos de recursos distintos: grupos de recursos personalizados y grupos de recursos del sistema.

Grupos de recursos definidos personalizados

Cree grupos de recursos personalizados en el Gestor de grupos de recursos. Utilice grupos de recursos personalizados para agrupar recursos basándose en su finalidad.

La tabla siguiente describe las acciones que puede realizar si tiene permiso de visualización para un grupo de recursos personalizados:

Tabla 240. Permiso de visualización para un grupo de recursos personalizados	
Acción	**Permiso disponible**
Ver el grupo de recursos personalizados y los recursos en el Gestor de grupos de recursos.	✓
Ver los recursos que forman parte del grupo de recursos personalizados en la ventana **Añadir aplicación** si también tiene el permiso de modificación para las aplicaciones.	✓

Tabla 240. Permiso de visualización para un grupo de recursos personalizados (continuación)	
Acción	**Permiso disponible**
Ver los recursos que forman parte del grupo de recursos personalizados en la aplicación predefinida **Mis componentes** si también tiene uno de los permisos de Panel de instrumentos del rendimiento de aplicaciones.	✓
Añadir recursos al grupo de recursos personalizados.	—
Suprimir recursos del grupo de recursos personalizados.	—

La tabla siguiente describe las acciones que puede realizar si tiene permiso de modificación para un grupo de recursos personalizados:

Tabla 241. Permiso de modificación para un grupo de recursos personalizados	
Acción	**Permiso disponible**
Asignar umbrales al grupo de recursos personalizados en el Editor de umbrales. **Nota:** Para asignar los umbrales, necesita también ser miembro de un rol que tenga permiso de visualización para el Editor de umbrales.	✓
Añadir recursos al grupo de recursos personalizados.	✓
Suprimir recursos del grupo de recursos personalizados.	✓

Grupos de recursos del sistema

Los grupos de recursos del sistema se han definido automáticamente como parte de la configuración del entorno de Cloud APM. Los grupos de recursos del sistema no se pueden crear de forma manual ni suprimir ni personalizar. Solo el permiso de visualización está disponible para los grupos de recursos del sistema, el permiso de modificación no está disponible.

Los grupos de recursos del sistema se definen para cada tipo de recurso en el momento en que Servidor de Cloud APM se vuelve reconocido para el recurso. Un grupo de recursos del sistema existe para cada tipo de recurso que está conectado a Servidor de Cloud APM.

Los agentes Cloud APM son un ejemplo de un recurso. Por ejemplo, la primera vez que descargue, instale e inicie un agente de Db2, se creará un grupo de recursos del sistema denominado Db2. Este grupo contiene todos los agente de Db2 que se han ido añadiendo posteriormente al entorno de Performance Management.

El grupo de recursos del sistema para cada tipo de recurso contiene todos los recursos de ese tipo incluidos los recursos de IBM Tivoli Monitoring. Si su entorno incluye IBM Tivoli Monitoring e IBM Cloud Application Performance Management, puede instalar IBM Cloud Application Performance Management Hybrid Gateway para proporcionar una vista de agentes de ambos dominios. Los grupos de recursos definidos por el sistema contienen agentes de los dos dominios. Para obtener más información, consulte “Integración con IBM Tivoli Monitoring V6.3 ” en la página 983.

Algunos grupos de recursos del sistema se basan en los agentes del subnodo. Aunque puede asignar los umbrales a los grupos de recursos del sistema basándose en los agentes del subnodo, no se muestran los sucesos en el Panel de instrumentos del rendimiento de aplicaciones. Los umbrales se

asignan a los grupos de recursos del sistema basándose en los agentes del subnodo para el reenvío de sucesos. Los grupos de recursos del sistema basándose en los agentes del subnodo tienen la descripción siguiente en el Gestor de grupos de recursos: ' los miembros de este grupo no se pueden añadir a una aplicación y no tienen los sucesos visualizados en la consola de Performance Management'. Para obtener más información, consulte “Gestor de grupos de recursos” en la página 1014.

La tabla siguiente describe las acciones que puede realizar si tiene permiso de visualización para un grupo de recursos del sistema:

Tabla 242. Permiso de visualización para un grupo de recursos del sistema

Acción	**Permiso disponible**
Ver el grupo de recursos del sistema en el Gestor de grupos de recursos.	✓
Ver los recursos que forman parte del grupo de recursos del sistema en la ventana **Añadir aplicación** si también tiene el permiso de modificación para las aplicaciones.	✓
Ver los recursos que forman parte del grupo de recursos del sistema en la aplicación predefinida **Mis componentes** si también tiene uno de los permisos de Panel de instrumentos del rendimiento de aplicaciones	✓
Asignar umbrales al grupo de recursos del sistema en el Editor de umbrales.	✓
Añadir recursos al grupo de recursos del sistema.	—
Suprimir recursos del grupo de recursos del sistema.	—

Trabajo con roles, usuarios y permisos
Utilice la página Control de accesos basado en roles para trabajar con roles, usuarios y permisos.

Antes de empezar
De forma alternativa, utilice la API de autorización para completar tareas de control de accesos basado en roles desde la línea de mandatos. Para obtener más información, consulte “Exploración de las API” en la página 1107.

Nota: Los grupos de usuarios no están soportados en Cloud APM.

Procedimiento

- Para filtrar la lista de roles, usuarios o grupos de usuarios que se muestra en la página Control de accesos basado en roles, siga estos pasos:
  a) Seleccione **Configuración del sistema > Control de accesos basado en roles**.
  b) Pulse dentro del recuadro de texto **Filtro** y teclee el texto parcial o completo por el que filtrar.
  Conforme escribe, las filas que no contienen lo que ha tecleado en el cuadro de texto se eliminan de la tabla.
  c) Para eliminar el filtro rápido, suprima el valor o pulse la "x".
  d) Para aplicar el filtro, pulse .
- Para crear un rol personalizado nuevo, siga estos pasos:
  a) Seleccione **Configuración del sistema > Control de accesos basado en roles**.

b) En la pestaña **Roles**, pulse . Se visualiza la página **Editor de roles**.

c) En la pestaña **Asignar usuarios a roles**, seleccione la pestaña **Grupos de usuarios** o en la pestaña **Usuarios individuales** y seleccione los usuarios y los grupos de usuarios que desea añadir al rol.

d) En la pestaña **Asignar permisos a roles**, seleccione la pestaña **Permisos de configuración del sistema** o la pestaña **Permisos de recursos** y seleccione los permisos que desea asignar al rol.

e) Pulse **Guardar**.

- Para editar un rol predeterminado o personalizado existente, siga estos pasos:

  a) Seleccione **Configuración del sistema > Control de accesos basado en roles**.

  b) En la pestaña **Roles**, pulse . Se visualiza la página **Editor de roles**.

  c) En la pestaña **Asignar usuarios a roles**, pulse en la pestaña **Grupos de usuarios** o en la pestaña **Usuarios individuales** y seleccione los usuarios o los grupos de usuarios que desea añadir al rol.

  d) En la pestaña **Asignar permisos a roles**, seleccione la pestaña **Permisos de configuración del sistema** o la pestaña **Permisos de recursos** y seleccione los permisos que desea asignar al rol.

  e) Pulse **Guardar**.

- Para suprimir un rol, siga estos pasos:

  a) Seleccione **Configuración del sistema > Control de accesos basado en roles**.

  b) En la pestaña **Roles**, seleccione el rol que desea suprimir y pulse . Se muestra un mensaje de confirmación; pulse **Aceptar**.

  Nota: Cuando suprime un rol, no se suprimen los usuarios que son miembros de ese rol. Siguen estando disponibles en la pestaña **Usuarios individuales** y el Administrador de roles los puede asignar a otro rol.

- Para editar los permisos para un usuario individual o un grupo de usuarios, siga estos pasos:

  a) Seleccione **Configuración del sistema > Control de accesos basado en roles**.

  b) En la pestaña **Usuario individual** o **Grupos de usuarios**, seleccione el usuario o el grupo de usuarios que desea editar y pulse . Se abre la página **Editor de usuario individual**.

  c) Seleccione el rol o los roles que desea asignar al usuario.

  d) Pulse **Guardar**.

- Para crear un archivo csv que resume los permisos para un usuario o un grupo de usuarios, siga estos pasos:

  a) En la pestaña **Usuario individual** o **Grupos de usuarios**, seleccione el usuario o el grupo de usuarios necesario y pulse . Se abre la página **Editor de usuario individual** o **Editor de grupo de usuarios**.

  b) Pulse **Resumen de exportación**.

  c) Seleccione **Guardar archivo** y pulse **Aceptar**.

  Un archivo csv que resume el permiso del usuario o el grupo de usuarios se guarda en la ubicación especificada.

Resultados

La asignación de roles y permisos surte efecto inmediatamente cuando pulsa **Guardar**.

Acceso y uso de la API Servicio de control de accesos basado en roles

Utilice la API Servicio de control de accesos basado en roles para gestionar el ciclo de vida de políticas de control de acceso basado en roles desde la línea de mandatos.

Acerca de esta tarea

Realice tareas de acceso basado en el rol como crear, ver, actualizar y suprimir roles. Añada y suprima un conjunto de usuarios o grupos de usuarios de un rol específico. Otorgue permisos a un rol específico. Visualice una lista de roles, usuarios, grupos de usuarios y permisos definidos en el sistema.

Puede crear scripts para automatizar tareas como la definición de nuevos roles y la asignación de usuarios, grupos de usuarios y permisos a estos roles.

Procedimiento

1. Complete del paso 1 al paso 9 del tema Exploración de las API.
   El paso 10 y el paso 11 proporcionan detalles adicionales.
2. Pulse **USE** y seleccione una clave, por ejemplo, **Key1**.

   Nota: Pulse **Ocultar** para mostrar el ID de cliente y el secreto de cliente. Anótelos porque, si está realizando llamadas de API con herramientas externas fuera del Explorador de API, son necesarios. A continuación, pulse **Mostrar** para ocultarlos.
3. Complete todas las cabeceras necesarias, indicadas con un asterisco.

   X-IBM-Service-Location
   * la cabecera es la ubicación geográfica de la suscripción, como por ejemplo na para Norteamérica

   Autorización
   * la cabecera es la serie codificada en base64 del ID y contraseña de IBM. Al codificar el ID y contraseña de IBM en la herramienta de codificación en based64, el formato debe ser *idIBM:contraseña*, por ejemplo, `Basic YXBtYWRtaW46YXBtcGFzcw==!`.
4. Debe incluir una cabecera de referenciador en todas las solicitudes POST, PUT y DELETE. El valor de la cabecera Referer es siempre:

   ```
   -H 'Referer: https://api.ibm.com'
   ```
5. Desplácese hasta localizar y pulse **Probar**.

Ejemplo

El ejemplo siguiente utiliza el mandato curl para crear un rol.

```
POST /1.0/authzn/roles
```

Nota: El cuerpo de la solicitud POST debe contener un objeto JSON que defina el rol según lo mostrado por el parámetro **-d**.

```
curl -X POST \
  https://api.ibm.com/perfmgmt/run/1.0/authzn/roles  \
  -H 'Referer: https://api.ibm.com' \
  -H 'authorization: Basic REPLACE_BASE64_ENCODED_STRING' \
  -H 'content-type: application/json' \
  -H 'x-ibm-client-id: REPLACE_KEY_VALUE' \
  -H 'x-ibm-client-secret: REPLACE_KEY_VALUE' \
  -d '{
    "description": "Your Role Description",
    "id": "/authzn/roles/Your_Role_Id",
    "label": "Your Role Name"
}'
```

Administración de los agentes

La instalación de IBM Cloud Application Performance Management tiene herramientas para gestionar los agentes de supervisión.

Algunas de estas herramientas también se utilizan durante la configuración inicial de los sistemas gestionados: “Utilización de mandatos de agente” en la página 184, “Página Configuración de agente” en

la página 189 y “Utilización de la ventana de IBM Cloud Application Performance Management en sistemas Windows” en la página 189.

Inicio de agentes mediante un usuario no root

Si desea iniciar agentes mediante usuarios diferentes, cree un grupo común en el sistema y convierta a cada usuario en un miembro de este grupo.

Antes de empezar

Si ha instalado y configurado el agente mediante el mismo usuario no root y desea iniciar el agente mediante el mismo usuario, no se necesita ninguna acción especial. Si ha instalado el agente mediante un usuario seleccionado y desea iniciar el agente mediante un usuario distinto, cree un grupo común en el sistema. Haga a todos los miembros usuarios de gestión de agentes de este grupo común. Transfiera la transferencia de todos los archivos de agente y directorios a este grupo.

Acerca de esta tarea

Una instalación, una actualización o una configuración generan un script de inicio automático. Este script (llamado `ITMAgentsN` o `rc.itmN`, en función del sistema operativo UNIX) contiene una entrada para cada aplicación en una instalación en particular. De forma predeterminada, todos los agentes se inician mediante acceso de usuario root. Para actualizar los scripts de inicio del sistema mediante un usuario no root, debe editar el archivo `dir_instalación/config/kcirunas.cfg`, que contiene un superconjunto de la sintaxis XML. Todas las secciones **productCode** del archivo `kcirunas.cfg` están inhabilitadas de forma predeterminada. Active una sección **productCode** para el agente eliminando el indicador de comentario del **!productCode**. Las secciones en forma de comentario o desactivadas se pasan por alto. Las secciones activadas o no comentario para las aplicaciones no instaladas se pasan por alto.

Procedimiento

1. Instale los agentes de supervisión en Linux o UNIX como se describe en “Instalación de agentes” en la página 130 en los sistemas AIX o “Instalación de agentes” en la página 138 en los sistemas Linux.
2. Opcional: Configure los agentes de supervisión en Linux o UNIX según sea necesario; consulte Capítulo 7, “Configuración del entorno”, en la página 165.
3. Ejecute el script `./secure.sh` con el nombre de grupo del usuario no root para proteger los archivos y establecer la propiedad del grupo de archivos en los archivos.
   Por ejemplo: **`./secure.sh -g db2iadm1`**
4. Para actualizar los scripts de inicio del sistema, realice los pasos siguientes:
   a) Actualice el archivo `dir_instalación/config/kcirunas.cfg`. Active las secciones **productCode** para los agentes. Para los agentes que no requieren un valor de instancia, especifique el código de producto, la instancia y el usuario, donde el valor de *código_producto* es el código de dos letras especificado en Tabla 11 en la página 185. Para los agentes que requieren un valor de instancia como, por ejemplo, el agente de supervisión de Db2 (código de producto: ud), especifique el código_producto, la instancia, el usuario y el nombre.
   Por ejemplo:

```
<productCode>ud</productCode>
<instance>
<name>db2inst1</name>
<user>db2inst1</user>
</instance>
<instance>
<name>db2inst2</name>
<user>root</user>
</instance>
```

   b) Ejecute el script siguiente con acceso de usuario root o de usuario sudo: *`dir_instalación`*`/bin/UpdateAutoRun.sh`

Qué hacer a continuación

Para obtener más información sobre el script **./secure.sh**, consulte Asegurar los archivos de instalación de agente.

Utilice el mismo ID de usuario para la instalación del agente y para las actualizaciones.

Umbrales de suceso para la supervisión de transacciones

Puede utilizar los umbrales de suceso para supervisar inmediatamente su entorno. Puede crear también umbrales de suceso personalizados que prueban determinadas condiciones y generan un suceso cuando los indicadores clave de rendimiento superan el umbral.

Sucesos de Supervisión de tiempo de respuesta

Los sucesos de tiempo de respuesta se crean cuando las transacciones web superan un umbral de **Tiempo de respuesta**.

Después de pulsar **Configuración del sistema** > **Gestor de umbrales**, seleccione **Tiempo de respuesta** como el **Tipo de origen de datos**. Todos los umbrales de suceso del entorno de Supervisión de tiempo de respuesta se aplican a todos los sistemas gestionados del mismo tipo.

Están disponibles los umbrales predefinidos siguientes para el agente de Supervisión de tiempo de respuesta.

Tabla 243. Umbrales de Supervisión de tiempo de respuesta

Umbral	Descripción	Fórmula
Response_Time_Availability_Crit	Un alto porcentaje de las transacciones web han fallado.	Si Estado de transacción de WRT.Percent_Failed es mayor que 0 y Estado de transacción de WRT.Transaction_Definition_Name no es igual a "Ignorar recursos", Response_Time_Availability_Crit es true
Response_Time_Availability_Warn	Un porcentaje moderado de las transacciones web han fallado.	Si Estado de transacción de WRT.Percent_Failed es mayor que 0 y Estado de transacción de WRT.Percent_Failed es menor que 10 y Estado de transacción de WRT.Transaction_Definition_Name no es igual a "Ignorar recursos", Response_Time_Availability_Warn es true
Response_Time_Critical	El porcentaje de las transacciones web con un tiempo de respuesta lento es alto.	Si Estado de transacción de WRT.Percent_Slow es mayor que 5 y Estado de transacción de WRT.Percent_Available es igual a 100 y Estado de transacción de WRT.Transaction_Definition_Name no es igual a "Ignorar recursos", Response_Time_Critical es true

Tabla 243. Umbrales de Supervisión de tiempo de respuesta (continuación)		
Umbral	**Descripción**	**Fórmula**
`Response_Time_Warning`	El porcentaje de las transacciones web con un tiempo de respuesta lento es moderado.	Si Estado de transacción de WRT.Percent_Slow es mayor que 1 y Estado de transacción de WRT.Percent_Slow es menor que 5 y Estado de transacción de WRT.Percent_Available es igual a 100 y Estado de transacción de WRT.Transaction_Definition_Name no es igual a "Ignorar recursos", Response_Time_Warning es true

Solicitudes buenas tienen un tiempo de respuesta inferior a 10 segundos. Las *Solicitudes lentas* tienen un tiempo de respuesta superior a 10 segundos. El valor de 10 segundos utilizado para determinar un tiempo de respuesta bueno versus uno lento no se puede configurar.

Sucesos de Rastreo de transacciones

Los sucesos de Rastreo de transacciones se crean cuando las transacciones de middleware superan un umbral de Rastreo de transacciones.

Para ver los umbrales de Rastreo de transacciones predeterminados, pulse **Configuración del sistema** > **Gestor de umbrales** y seleccione **Rastreo de transacciones** como el **Tipo de origen de datos**.

Consejo: Puede crear sus propios umbrales de Rastreo de transacciones si es necesario.

Están disponibles los umbrales predefinidos siguientes para las transacciones de middleware.

Tabla 244. Umbrales de Rastreo de transacciones		
Umbral	**Descripción**	**Fórmula**
`Interaction_Avail_Critical`	Un alto porcentaje de las interacciones de middleware han fallado.	Si DATOS DE AGREGADOS DE INTERACCIONES DE KTE.PERCENTAGE_FAILED es mayor que 10, Interaction_Avail_Critical es true
`Interaction_Avail_Warning`	Un porcentaje moderado de las interacciones de middleware han fallado.	SI DATOS DE AGREGADOS DE INTERACCIONES DE KTE.PERCENTAGE_FAILED es mayor que 0 y DATOS DE AGREGADOS DE INTERACCIONES DE KTE.PERCENTAGE_FAILED es menor o igual que 10, `Interaction_Avail_Warning` es true
`Interaction_Time_Critical`	El porcentaje de las interacciones de middleware con un tiempo total lento es alto.	Si DATOS DE AGREGADOS DE INTERACCIONES DE KTE.PERCENTAGE_SLOW es mayor o igual que 5 y DATOS DE AGREGADOS DE INTERACCIONES DE KTE.PERCENTAGE_FAILED es igual a 0, Interaction_Time_Critical es true

Tabla 244. Umbrales de Rastreo de transacciones (continuación)

Umbral	Descripción	Fórmula
`Interaction_Time_Warning`	El porcentaje de las interacciones de middleware con un tiempo total lento es moderado.	Si DATOS DE AGREGADOS DE INTERACCIONES DE KTE.PERCENTAGE_SLOW es mayor que 1 y DATOS DE AGREGADOS DE INTERACCIONES DE KTE.PERCENTAGE_SLOW es menor que 5 y DATOS DE AGREGADOS DE INTERACCIONES DE KTE.PERCENTAGE_FAILED es igual a 0, Interaction_Time_Warning es true
`Transaction_Avail_Critical`	Un alto porcentaje de las transacciones de middleware han fallado.	Si DATOS DE AGREGADOS DE TRANSACCIONES DE KTE_FAILED es mayor que 10, Transaction_Avail_Critical es true
`Transaction_Avail_Warning`	Un porcentaje moderado de las transacciones de middleware han fallado.	SI DATOS DE AGREGADOS DE TRANSACCIONES DE KTE.PERCENTAGE_FAILED es mayor que 0 y DATOS DE AGREGADOS DE TRANSACCIONES DE KTE.PERCENTAGE_FAILED es menor o igual que 10, `Transaction_Avail_Warning` es true
`Transaction_Time_Critical`	El porcentaje de las transacciones de middleware con un tiempo total lento es alto.	Si DATOS DE AGREGADOS DE TRANSACCIONES DE KTE.PERCENTAGE_SLOW es mayor o igual que 5 y DATOS DE AGREGADOS DE TRANSACCIONES DE KTE.PERCENTAGE_FAILED es igual a 0, Transaction_Time_Critical es true
`Transaction_Time_Warning`	El porcentaje de las transacciones de middleware con un tiempo total lento es moderado.	Si DATOS DE AGREGADOS DE TRANSACCIONES DE KTE.PERCENTAGE_SLOW es mayor que 1 y DATOS DE AGREGADOS DE TRANSACCIONES DE KTE.PERCENTAGE_SLOW es menor que 5 y DATOS DE AGREGADOS DE TRANSACCIONES DE KTE.PERCENTAGE_FAILED es igual a 0, Transaction_Time_Warning es true

Solicitudes buenas tienen un tiempo de respuesta inferior a 10 segundos. Las *Solicitudes lentas* tienen un tiempo de respuesta superior a 10 segundos. El valor de 10 segundos utilizado para determinar un tiempo de respuesta bueno versus uno lento no se puede configurar.

Creación de umbrales para generar sucesos para la supervisión de transacciones

Utilice el Gestor de umbrales para crear umbrales de transacciones. Los umbrales se utilizan para comparar el valor muestreado de un atributo con el valor establecido en el umbral. Si el valor muestreado satisface la comparación, se genera un suceso de transacción.

Acerca de esta tarea

Puede supervisar cuando las aplicaciones notifican condiciones específicas utilizando umbrales. Para obtener más información sobre los umbrales predeterminados para la supervisión de transacciones, consulte “Umbrales de suceso para la supervisión de transacciones ” en la página 1048.

Puede crear umbrales adicionales para supervisar otros aspectos de una transacción. Por ejemplo, puede crear un umbral para supervisar si la tasa de suceso de transacción de middleware baja. A continuación, si la tasa de suceso de transacción está por debajo del umbral especificado, se genera un suceso.

Procedimiento

Para crear un umbral y asociarlo a una o varias transacciones, realice las tareas siguientes:

1. En la barra de navegación, pulse **Configuración del sistema** > **Gestor de umbrales**. Establezca el **Tipo de origen de datos** como **Rastreo de transacciones**.
2. Pulse Añadir para crear un nuevo umbral.
3. Establezca una gravedad para el suceso que supera este umbral.
4. Para asociar el umbral a una transacción, establezca los valores siguientes:
   - Conjunto de datos - `DATOS DE AGREGADOS DE TRANSACCIONES DE KTE`
   - Elemento de visualización - `Resource_Value`
   - Operador lógico - `And (&)`
5. De format alternativa, para asociar el umbral con una interacción, establezca los valores siguientes:
   - Conjunto de datos - `DATOS DE AGREGADOS DE INTERACCIÓN DE KTE`
   - Elemento de visualización - `Valor_Recurso_Origen`
   - Operador lógico - `And (&)`
6. Pulse **Añadir** para añadir una condición. En el recuadro **Añadir condición**, seleccione un atributo y un operador, a continuación, especifique un valor de umbral.

   Por ejemplo, para añadir una condición de umbral que genere un suceso de transacción cuando el número de transacciones por minuto esté por debajo de 100, establezca los valores siguientes y pulse **Aceptar**:
   - Atributo - `Transaction_Rate`
   - Operador - `Menor que`
   - Valor - `100`

   Repita este paso para añadir más condiciones al umbral si es necesario.
7. En la sección Asignación de grupos, seleccione `Rastreo de transacciones` para asignar el umbral a ese grupo de recursos.
8. Pulse **Guardar**.

Resultados

Habrá creado un umbral y lo habrá asociado a una transacción o interacción. Cuando se cumplen las condiciones de umbral, se genera un suceso. Puede supervisar los sucesos en la pestaña Sucesos del panel de instrumentos de rendimiento de aplicaciones.

Ejemplo

Para crear umbrales para que el agente Supervisión de tiempo de respuesta supervise otros aspectos de una transacción web además de los valores predeterminados:

1. En el Gestor de umbrales, establezca el **Tipo de origen de datos** como **Tiempo de respuesta**.
2. Al añadir el umbral, utilice estos valores:
   - Conjunto de datos - `Estado de transacción de WRT`

- Elemento de visualización - `Aplicación`
- Operador lógico - `And (&)`
- Asignación de grupos - `Tiempo de respuesta web`

Gestión de sucesos de agente de sistema operativo

Puede configurar el agente de sistema operativo para gestionar sucesos.

Filtrado y resumen de sucesos

Utilice las opciones de filtrado y resumen de sucesos que ha establecido en el archivo de configuración (`.conf`) para controlar cómo maneja el agente de sistema operativo los sucesos duplicados.

Cuando se supervisa un registro, un suceso puede aparecer varias veces rápidamente. Por ejemplo, este registro repetido puede producirse cuando la aplicación que genera el registro encuentra un error y registra este error continuamente hasta que se resuelve el umbral. Cuando se produce este tipo de registro, se envía un número excesivo de sucesos a la infraestructura de Performance Management. El volumen de sucesos tiene un impacto negativo en el rendimiento.

Nota: Los procedimientos de detección y de resumen de sucesos sólo están soportados para sucesos que se envían a Performance Management. No puede completar estos procedimientos para los sucesos enviados a OMNIbus por EIF.

Detección y filtrado de sucesos duplicados

Puede configurar el agente de sistema operativo para gestionar sucesos duplicados.

Para aliviar el problema de tener varios sucesos duplicados, debe definir qué constituye un suceso duplicado utilizando la etiqueta `DupDetectionKeyAttributes` del archivo `.conf`. En una lista separada por comas, incluya uno o más atributos definidos de Performance Management que desea utilizar para determinar si un suceso se considera duplicado. En el ejemplo siguiente, los sucesos con el mismo mensaje y el mismo `CustomSlot1` deben considerarse duplicados:

```
DupDetectionKeyAttributes=msg,CustomSlot1
```

Los sucesos duplicados se detectan a partir de atributos de Performance Management. Por lo tanto, si desea que la detección de duplicados se base en determinados atributos que defina, realice los pasos siguientes:

1. Correlacione el valor del atributo con un atributo de Performance Management.
2. Correlacione ese atributo de Performance Management con la etiqueta `DupDetectionKeyAttributes` del archivo `.conf`.

Utilizando el ejemplo siguiente, en el que los atributos importantes, `eventclass` y `eventid`, se correlacionan con *CustomSlot1* y *CustomSlot2*:

```
REGEX BaseAuditEvent
^([A-Z][a-z]{2} [0-9]{1,2} [0-9]{1,2}:[0-9]{2}:[0-9]{2}
 [0-9] {4}) [0-9] (\S+) (\S+) \
Microsoft-Windows-Security-Auditing (\S+) ([0-9]+) (.*)
timestamp $1
severity $2
eventclass $3 CustomSlot1
eventkeywords $4
eventid $5 CustomSlot2
msg $6
END
```

si desea especificar determinados sucesos como sucesos duplicados, en el archivo `.conf`, correlacione los atributos de Performance Management con la etiqueta `DupDetectionKeyAttributes` tal como se muestra a continuación:

```
DupDetectionKeyAttributes=CustomSlot1,CustomSlot2
```

Nota:

1. Los nombres de atributo `CustomSlot` son sensibles a mayúsculas y minúsculas y, por tanto, debe especificar los nombres exactamente como se muestra en el ejemplo anterior.
2. Si no se proporciona una lista de atributos, los valores predeterminados serán `Class` y `Logname`.

El agente considerará sucesos duplicados los sucesos en los que coincidan estos atributos.

Puesto que la detección de duplicados es global, se recomienda seleccionar un conjunto de atributos personalizados para utilizarlos como claves y utilizarlos de este modo en todas las sentencias de formato. Por ejemplo, utilice los atributos 1-3 para las claves. Si un formato sólo necesita una clave pero también necesita más atributos, utilice el atributo uno para que contenga el valor de nombre y los atributos cuatro a n para que contengan los otros datos.

Intervalo de resumen
El procedimiento de detección de duplicados opera durante un período de tiempo denominado Intervalo de resumen.

Los sucesos duplicados se cuentan durante este intervalo y, posteriormente, se restablecen cuando expira el intervalo. El contador vuelve a iniciar el recuento empezando por 0 al principio de cada nuevo intervalo de resumen.

El agente envía un suceso de resumen para cada conjunto de sucesos que supervisa durante el intervalo. El suceso de resumen contiene los valores de atributo del primer suceso que coincide. El suceso de resumen también contiene un número que indica cuántos duplicados de dicho suceso se han producido durante el intervalo de resumen.

El intervalo de resumen se establece en el archivo de configuración (`.conf`) tal como se muestra en el ejemplo siguiente:

```
EventSummaryInterval=300
```

El valor que se asigna al intervalo de resumen es en segundos, por lo tanto, en este ejemplo, el intervalo de resumen es de 5 minutos.

Filtrado de sucesos
Si el filtrado de sucesos está en ejecución, el valor de EventFloodThreshold en el archivo (`.conf`) indica al agente cuándo enviar un suceso.

En la tabla siguiente se muestran los valores de EventFloodThreshold:

Tabla 245. Valores de EventFloodThreshold

Valores de EventFloodThreshold	**Descripción**
send_all	El valor *send_all* es el valor predeterminado. Se envían todos los sucesos, aunque sean sucesos duplicados.
send_none	El valor *send_none* significa que no se envían sucesos individuales. Sólo se envían los sucesos de resumen.
send_first	Utilice el valor *send_first* para enviar el primer suceso en cuanto se encuentre. Si se producen duplicados de ese primer suceso dentro de un tiempo especificado, los duplicados subsiguientes de ese primer suceso no se enviarán. Para obtener más información, consulte “Intervalo de resumen” en la página 1053.

Tabla 245. Valores de EventFloodThreshold (continuación)	
Valores de EventFloodThreshold	**Descripción**
n integer	Utilice el valor *n* integer para enviar sólo cada ocurrencia *n* de un suceso (por ejemplo, cada quinto duplicado) durante un determinado período de tiempo. Para obtener más información, consulte "Intervalo de resumen" en la página 1053.

Atributos de resumen
Los atributos Tipo de suceso y Recuento de apariciones se utilizan para ayudar a resumir sucesos.

Cuando se habilita el resumen de sucesos, tienen sentido los atributos Tipo de suceso y Recuento de apariciones. El atributo Tipo de suceso indica el tipo del suceso, que puede ser un *Suceso* o un *Suceso de resumen*. Los sucesos generales que se corresponden con los registros que se encuentran en el registro de modo unívoco, se etiquetan como *Suceso*. Los sucesos de resumen que se envían al final del intervalo de resumen se etiquetan como *Suceso de resumen*.

El atributo Recuento de apariciones indica la cantidad total de registros duplicados que se han encontrado para el suceso. Los sucesos de resumen incluyen este recuento porque muestra el número de sucesos recibidos que coincidían con el suceso de resumen durante el intervalo de resumen anterior.

Umbrales y sucesos de resumen

Independientemente del valor del filtro tal como se describe en "Filtrado de sucesos" en la página 1053, siempre obtendrá los sucesos de resumen al final de cada intervalo de resumen, para cualquier suceso que se haya producido al menos una vez durante ese intervalo. Si no espera los sucesos de resumen, los umbrales pueden activarse accidentalmente. Para evitar este desencadenamiento accidental de un umbral, incluya una cláusula en el umbral para *Tipo de suceso== Suceso* o *Tipo de suceso!= Resumen de sucesos*.

Registro de sucesos de Windows
El agente de sistema operativo utiliza el archivo .conf para supervisar sucesos del registro de sucesos de Windows.

El agente de sistema operativo continúa utilizando la opción `WINEVENTLOGS` del archivo de configuración `(.conf)` para supervisar sucesos del registro de sucesos de Windows. El agente supervisa una lista separada por comas de registros de sucesos tal como se muestra en el ejemplo siguiente:

```
WINEVENTLOGS=System,Security,Application
```

El agente de sistema operativo también continúa utilizando el valor `WINEVENTLOGS=All`. El valor `All` hace referencia a los registros de sucesos estándar siguientes: Seguridad, Aplicación, Sistema, Directorio, Sistema de nombres de dominio (DNS) y Servicio de réplica de archivos (FRS) que se suministran con las versiones de Windows anteriores a 2008. No obstante, no se comprueban todos los registros de sucesos del sistema.

La etiqueta del archivo de configuración `UseNewEventLogAPI` permite al registro de sucesos (registros de sucesos de Windows 2008 o posterior) acceder a todos los nuevos registros añadidos por Microsoft, y todos los registros de sucesos de Windows creados por otras aplicaciones o por el usuario. Los nuevos registros se listan en la palabra clave `WINEVENTLOGS`.

En el ejemplo siguiente, la etiqueta `UseNewEventLogAPI` se establece en `y`.

```
UseNewEventLogAPI=y
WINEVENTLOGS=Microsoft-Windows-Hyper-V-Worker-Admin
```

En este ejemplo, `Microsoft-Windows-Hyper-V/Admin` se supervisa en un sistema Windows que tiene el rol Hyper-V.

En el registro de sucesos de Windows, cada suceso tiene los campos siguientes en este orden:

- La fecha en el formato siguiente: mes, día, hora y año.
- La categoría de suceso como un entero
- Nivel de suceso
- ID de seguridad de Windows. Los espacios del ID de seguridad de Windows se sustituyen por un guión bajo si `SpaceReplacement=TRUE` en el archivo de configuración (`.conf`).

  Nota: `SpaceReplacement=TRUE` es el valor predeterminado si establece `UseNewEventLogAPI` en y en el archivo (`.conf`) (designado que está utilizando el registro de sucesos).
- Origen de Windows. Los espacios del origen de Windows se sustituyen por un guión bajo si `SpaceReplacement=TRUE` en el archivo de configuración (`.conf`).
- Palabras clave del registro de sucesos de Windows. Los espacios en las palabras clave del registro de sucesos de Windows se sustituyen por un guión bajo si `SpaceReplacement=TRUE` en el archivo de configuración (`.conf`).

  Nota: El campo de palabras clave que se describe aquí es nuevo para la versión del registro de sucesos de Windows 2008. No existía en el registro de sucesos anterior y por lo tanto su presencia le impide reutilizar directamente sus sentencias con formato del registro de sucesos anterior. Éstas se deben modificar para tener en cuenta este campo adicional.
- Identificador de sucesos de Windows
- Texto del mensaje

Por ejemplo, cuando un usuario administrativo inicia la sesión en un sistema Windows 2008, se genera un suceso en el registro Seguridad que indica los privilegios que están asignados a la nueva sesión de usuario:

```
Mar 22 13:58:35 2011 1 Information N/A Microsoft-Windows-
Security-Auditing Audit_Success 4672 Special privileges assigned to new logon.
S-1-5-21-586564200-1406810015-1408784414-500    Account Name:
Administrator   Account Domain:     MOLDOVA     Logon ID:
0xc39cb8e    Privileges:        SeSecurityPrivilege
SeBackupPrivilege          SeRestorePrivilege
SeTakeOwnershipPrivilege            SeDebugPrivilege
SeSystemEnvironmentPrivilege            SeLoadDriverPrivilege
SeImpersonatePrivilege
```

Para capturar todos los sucesos creados por el origen de sucesos `Microsoft-Windows-Security-Auditing`, se debe escribir una sentencia de formato como seindica:

```
REGEX BaseAuditEvent
^([A-Z][a-z]{2} [0-9]{1,2} [0-9]{1,2}:[0-9]{2}:[0-9]{2} [0-9]
{4}) [0-9] (\S+) (\S+) Microsoft-Windows-Security-Auditing (\S+)
([0-9]+) (.*)
timestamp $1
severity $2
login $3
eventsource "Microsoft-Windows-Security-Auditing"
eventkeywords $4
eventid $5
msg $6
END
```

Para el suceso de ejemplo anterior, en el ejemplo siguiente se indican los valores asignados a los atributos:

```
timestamp=Mar 22 13:58:35 2011
severity=Information
login=N/A
eventsource=Microsoft-Windows-Security-Auditing
eventid=4672
msg="Special privileges assigned to new logon.
S-1-5-21-586564200-1406810015-1408784414-500    Account Name:
Administrator   Account Domain:     MOLDOVA     Logon ID:
0xc39cb8e    Privileges:        SeSecurityPrivilege
SeBackupPrivilege          SeRestorePrivilege
SeTakeOwnershipPrivilege            SeDebugPrivilege
```

```
SeSystemEnvironmentPrivilege            SeLoadDriverPrivilege
SeImpersonatePrivilege
```

Puesto que es difícil de prever qué aspecto tendrán exactamente estos sucesos, un método útil para grabar las expresiones regulares es capturar los sucesos reales en un archivo. A continuación, puede examinar el archivo, elegir los sucesos que desea que el agente capture y grabar expresiones regulares que coincidan con estos sucesos. Para capturar todos los sucesos del registro de sucesos de Windows, utilice los siguientes pasos:

1. Cree un archivo de formato que contenga sólo un patrón que no coincida con nada, como se muestra en el ejemplo siguiente:

   ```
   REGEX NoMatch
   Esto no coincide con nada
   END
   ```

2. Añada el valor siguiente al archivo de configuración (`.conf`):

   ```
   UnmatchLog=C:/temp/evlog.unmatch
   ```

3. Ejecute el agente y capture algunos sucesos de ejemplo.

Correlación de sucesos
La interfaz de Tivoli Event Integration Facility (EIF) se utiliza para reenviar sucesos de situación a Tivoli Netcool/OMNIbus, Tivoli Enterprise Console, o Operations Analytics - Log Analysis.

Los sucesos de EIF especifican una clase de suceso y los datos de suceso se especifican como pares nombre-valor que identifican el nombre de un atributo de suceso y el valor para el atributo. Una clase de suceso puede tener subclases. Performance Management proporciona las definiciones de clase de suceso base y un conjunto de atributos de base que se incluyen en todos los sucesos de supervisión. Los agentes amplían las clases de suceso base para definir las subclases que incluyen atributos específicos de agente. Para sucesos del archivo de registro de agente de sistema operativo, las clases de sucesos corresponden a los grupos de atributos del agente, y los atributos específicos de agente corresponden a los atributos del grupo de atributos.

Para los sucesos que se generan mediante los umbrales en el grupo de atributos LFAProfiles, los sucesos se envían mediante la clase de suceso ITM_KLO_LFAPROFILES. Esta clase de suceso contiene los atributos siguientes:

- node: STRING
- timestamp: STRING
- subnode_msn: STRING
- subnode_affinity: STRING
- subnode_type: STRING
- subnode_resource_name: STRING
- subnode_version: STRING
- subnode_config_file: STRING
- subnode_description: STRING
- subnode_description_enum: STRING

Para los sucesos que se generan mediante los umbrales en el grupo de atributos de Estadísticas de regex de archivo de registro, los sucesos se envían mediante la clase de suceso ITM_KLO_LOG_FILE_REGEX_STATISTICS. Esta clase de suceso contiene los atributos siguientes:

- node: STRING
- timestamp: STRING
- table_name: STRING

- attrib_name: STRING
- filter_number: INTEGER
- average_processor_time: REAL
- average_processor_time_enum: STRING
- total_processor_time: REAL
- total_processor_time_enum: STRING
- max_processor_time: REAL
- max_processor_time_enum: STRING
- min_processor_time: REAL
- min_processor_time_enum: STRING
- filter_count: REAL
- filter_count_matched: REAL
- filter_count_unmatched: REAL
- regex_pattern: STRING
- last_matched_time: STRING
- last_matched_time_enum: STRING
- last_unmatched_time: STRING
- last_unmatched_time_enum: STRING
- result_type: INTEGER
- result_type_enum: STRING

Para los sucesos que se generan mediante los umbrales en el grupo de atributos de Estado de archivo de registro, los sucesos se envían mediante la clase de suceso ITM_KLO_LOG_FILE_STATUS. Esta clase de suceso contiene los atributos siguientes:

- node: STRING
- timestamp: STRING
- table_name: STRING
- file_name: STRING
- regex_pattern: STRING
- file_type: INTEGER
- file_type_enum: STRING
- file_status: INTEGER
- file_status_enum: STRING
- num_records_matched: INTEGER
- num_records_not_matched: INTEGER
- num_records_not_matched_enum: STRING
- num_records_processed: INTEGER
- current_file_position: REAL
- current_file_position_enum: STRING
- current_file_size: REAL

- current_file_size_enum: STRING
- last_modification_time: STRING
- last_modification_time_enum: STRING
- codepage: STRING

Para los sucesos que se generan mediante los umbrales en el grupo de atributos Sucesos de archivo de registro, los sucesos se envían mediante la clase de suceso ITM_KLO_LOGFILEEVENTS. Esta clase de suceso contiene los atributos siguientes:

- node: STRING
- timestamp: STRING
- klo_class: STRING
- logname: STRING
- eifevent: STRING
- klo_msg: STRING
- customslot1: STRING
- customslot2: STRING
- customslot3: STRING
- customslot4: STRING
- customslot5: STRING
- customslot6: STRING
- customslot7: STRING
- customslot8: STRING
- customslot9: STRING
- customslot10: STRING
- occurrence_count: INTEGER
- occurrence_count_enum: STRING
- event_type: INTEGER
- event_type_enum: STRING
- custominteger1: REAL
- custominteger1_enum: STRING
- custominteger2: REAL
- custominteger2_enum: STRING
- custominteger3: REAL
- custominteger3_enum: STRING
- remotehost: STRING

Para los sucesos que se generan mediante los umbrales en el grupo de atributos de Sucesos de perfil de archivo de registro, los sucesos se envían mediante la clase de suceso ITM_KLO_LOGFILEPROFILEEVENTS. Esta clase de suceso contiene los atributos siguientes:

- node: STRING
- timestamp: STRING
- klo_class: STRING

- logname: STRING
- eifevent: STRING
- klo_msg: STRING
- customslot1: STRING
- customslot2: STRING
- customslot3: STRING
- customslot4: STRING
- customslot5: STRING
- customslot6: STRING
- customslot7: STRING
- customslot8: STRING
- customslot9: STRING
- customslot10: STRING
- occurrence_count: INTEGER
- occurrence_count_enum: STRING
- event_type: INTEGER
- event_type_enum: STRING
- custominteger1: REAL
- custominteger1_enum: STRING
- custominteger2: REAL
- custominteger2_enum: STRING
- custominteger3: REAL
- custominteger3_enum: STRING
- remotehost: STRING

Para los sucesos que se generan mediante los umbrales en el grupo de atributos de Estatus de objeto de rendimiento, los sucesos se envían mediante la clase de suceso ITM_KLO_PERFORMANCE_OBJECT_STATUS. Esta clase de suceso contiene los atributos siguientes:

- node: STRING
- timestamp: STRING
- query_name: STRING
- object_name: STRING
- object_type: INTEGER
- object_type_enum: STRING
- object_status: INTEGER
- object_status_enum: STRING
- error_code: INTEGER
- error_code_enum: STRING
- last_collection_start: STRING
- last_collection_start_enum: STRING

- last_collection_finished: STRING
- last_collection_finished_enum: STRING
- last_collection_duration: REAL
- average_collection_duration: REAL
- average_collection_duration_enum: STRING
- refresh_interval: INTEGER
- number_of_collections: INTEGER
- cache_hits: INTEGER
- cache_misses: INTEGER
- cache_hit_percent: REAL
- intervals_skipped: INTEGER

Para los sucesos que se generan mediante los umbrales en el grupo de atributos de Estatus de objeto de rendimiento pro, los sucesos se envían mediante la clase de suceso ITM_KLO_PRO_PERFORMANCE_OBJECT_STATUS. Esta clase de suceso contiene los atributos siguientes:

- node: STRING
- timestamp: STRING
- query_name: STRING
- object_name: STRING
- object_type: INTEGER
- object_type_enum: STRING
- object_status: INTEGER
- object_status_enum: STRING
- error_code: INTEGER
- error_code_enum: STRING
- last_collection_start: STRING
- last_collection_start_enum: STRING
- last_collection_finished: STRING
- last_collection_finished_enum: STRING
- last_collection_duration: REAL
- average_collection_duration: REAL
- average_collection_duration_enum: STRING
- refresh_interval: INTEGER
- number_of_collections: INTEGER
- cache_hits: INTEGER
- cache_misses: INTEGER
- cache_hit_percent: REAL
- intervals_skipped: INTEGER

Para los sucesos que se generan mediante los umbrales en el grupo de atributos de Estatus de agrupación de hebras, los sucesos se envían mediante la clase de suceso ITM_KLO_THREAD_POOL_STATUS. Esta clase de suceso contiene los atributos siguientes:

- node: STRING
- timestamp: STRING
- thread_pool_size: INTEGER
- thread_pool_size_enum: STRING
- thread_pool_max_size: INTEGER
- thread_pool_max_size_enum: STRING
- thread_pool_active_threads: INTEGER
- thread_pool_active_threads_enum: STRING
- thread_pool_avg_active_threads: REAL
- thread_pool_avg_active_threads_enum: STRING
- thread_pool_min_active_threads: INTEGER
- thread_pool_min_active_threads_enum: STRING
- thread_pool_max_active_threads: INTEGER
- thread_pool_max_active_threads_enum: STRING
- thread_pool_queue_length: INTEGER
- thread_pool_queue_length_enum: STRING
- thread_pool_avg_queue_length: REAL
- thread_pool_avg_queue_length_enum: STRING
- thread_pool_min_queue_length: INTEGER
- thread_pool_min_queue_length_enum: STRING
- thread_pool_max_queue_length: INTEGER
- thread_pool_max_queue_length_enum: STRING
- thread_pool_avg_job_wait: REAL
- thread_pool_avg_job_wait_enum: STRING
- thread_pool_total_jobs: INTEGER
- thread_pool_total_jobs_enum: STRING

Gestión de transacciones sintéticas y sucesos con Website Monitoring

Cree transacciones sintéticas que supervisen el rendimiento y la disponibilidad de aplicaciones internas externas y de aplicaciones web públicas en ubicaciones diferentes.

Cree una *transacción sintética* en el Gestor de scripts sintéticos. Genere scripts sencillos en el Gestor de scripts sintéticos para probar la disponibilidad de una aplicación, o utilice Selenium IDE para grabar scripts sintéticos que dupliquen acciones de usuario diferentes con una aplicación. A continuación, configure una transacción sintética para que reproduzca su script en intervalos y ubicaciones de reproducción específicos.

Importante: Solo los usuarios existentes del complemento IBM Website Monitoring on Cloud pueden utilizar el Agente de Synthetic Playback y el Gestor de scripts sintéticos. Website Monitoring ha sido sustituido por IBM Cloud Availability Monitoring para el release de agosto de 2017. Para obtener más información, consulte “Acerca de Availability Monitoring” en la página 1081.

Las ubicaciones de reproducción disponibles son las ubicaciones en las que ha instalado Monitoring Agent for Synthetic Playback y los 15 puntos de presencia (PoP) que se suministran para aplicaciones web orientadas al público. Están disponibles PoPs para las ubicaciones siguientes:

- Amsterdam
- Chennai
- Dallas
- Frankfurt
- Hong Kong
- London
- Melbourne
- México
- París
- San José
- Sao Paulo
- Singapur
- Tokio
- Toronto
- Washington

Cree umbrales y grupos de recursos para que surjan sucesos y se notifique a los interesados cuando las aplicaciones son lentas o no están disponibles. Vea datos de rendimiento y genere informes históricos en Panel de instrumentos del rendimiento de aplicaciones.

Si supervisa el tiempo de respuesta de usuario final para una aplicación con el agente de Tiempo de respuesta, puede ver los ICR para las transacciones sintéticas y para el usuario final en el Panel de instrumentos del rendimiento de aplicaciones. Añada las transacciones sintéticas como componentes a la aplicación que esté supervisando con el agente de Tiempo de respuesta.

Nota: Para trabajar en el Gestor de scripts sintéticos, debe ser miembro de un rol que tenga permiso de vista para el Gestor de scripts sintéticos y para la Configuración de agente. Para obtener más información, consulte “Roles y permisos” en la página 1036.

Grabación de scripts sintéticos

Grabe un script sintético utilizando el navegador web Firefox y el complemento Selenium IDE.Con Selenium IDE, puede grabar las acciones de usuario en una página web, como cargar una página, pulsar un enlace o seleccionar un objeto. Cuando Selenium IDE graba, genera un mandato para cada acción de usuario en un script. A continuación, utilizando el Gestor de scripts sintéticos, puede configurar scripts para simular el comportamiento de usuario en el sitio web, a intervalos establecidos y en distintas ubicaciones.

Antes de empezar

Debe utilizar el navegador web Firefox al grabar los scripts

Selenium IDE está disponible solo como un complemento de Firefox.Si Selenium IDE no está instalado o en ejecución, realice los pasos siguientes:

1. Asegúrese de que está ejecutando una versión de Firefox 60 o posterior que dé soporte a Selenium IDE 3.2.X o 3.3.X. Si tiene una versión posterior de Selenium IDE, no estará soportada; debe desinstalarla e instalar la versión 3.2.X o 3.3.X.

   Nota: De forma predeterminada, el IDE de Selenium se actualiza automáticamente después de instalar la versión 3.2.X o 3.3.X. Desactive las actualizaciones automáticas para el IDE de Selenium para evitar actualizaciones de versión.

2. Descargue e instale el IDE de Selenium 3.2.X o 3.3.X desde la página de inicio de **Selenium** (https://addons.mozilla.org/firefox/addon/selenium-ide/versions/). Permita que Selenium IDE instale todos los plug-ins.
3. Cuando esté instalado Selenium IDE, reinicie Firefox.
4. Vaya a la página web que desea probar y cierre todas las demás pestañas. Para abrir Selenium IDE, pulse **Herramientas** > **Selenium IDE**. En la ventana **Selenium IDE**, asegúrese de que el campo **URL base** contiene el URL de la página web mostrada. Selenium IDE empezará a grabar todas las acciones de usuario en la página web mostrada.

Formato del script de Selenium .side

Los scripts creados con versiones más recientes de Selenium utilizan el formato `.side`. Con Selenium IDE 3.2.X o 3.3.X, puede importar scripts más antiguos creados con el formato `.html` y guardarlos en formato `.side`. Para obtener más información, consulte "Actualización de scripts desde versiones anteriores de Selenium IDE" en la página 1066.

Si va a utilizar scripts de Selenium `.side` , primero debe instalar estas actualizaciones:

- El Agente de Synthetic Playback de IBM Cloud Application Performance Management V8.1.4.0 arreglo temporal 5 o posterior en los sistemas donde haya instalado el Agente de Synthetic Playback.
- Póngase en contacto con IBM para asegurarse de que su suscripción de Cloud APM se ha actualizado al arreglo temporal 8 de IBM Cloud Application Performance Management, Private Cloud APM V8.1.4.0 Server o posterior.
- Si utiliza un punto de presencia (PoP) privado de Availability Monitoring, compruebe que el número de compilación de PoP sintético sea `APM_201903090832` o posterior especificando el mandato **`cat build.info`** desde el directorio de instalación de PoP. Las versiones de compilación anteriores no dan soporte al formato `.side`.

Los arreglos temporales para Cloud APM V8.1.4.0 están disponibles para su descarga desde IBM Support > Fix Central > IBM APM 8.1.4.0.

Acerca de esta tarea

En esta tarea, realizará acciones de usuario en una página web y utilizará Selenium IDE para grabar estas acciones como mandatos en un script simple. Puede utilizar los scripts para supervisar el rendimiento y la disponibilidad de la aplicación web en el Panel de instrumentos del rendimiento de aplicaciones.

Procedimiento

Realice los pasos siguientes para grabar un script de acciones de usuario en una página web:

1. Pulse **Grabar** para iniciar la grabación de un script. Realice acciones de usuario en la página web, como pulsar un enlace.

   Para cada acción de usuario en una página web, Selenium IDE graba un mandato y lo añade a un script.

   Por ejemplo, complete las acciones siguientes para registrar cuando un usuario carga la página web IBM Marketplace y navega a una prueba gratuita de Cloud APM, en un script:

Tabla 246. Acciones de usuario grabadas y mandatos de Selenium IDE

Acción de usuario	**Mandatos añadidos al script**
Para registrar cuándo se abre la página web Cloud APM en el sitio web IBM Marketplace, abra la página web IBM Marketplace. Pulse con el botón derecho del ratón en cualquier lugar de la página web visualizada y seleccione **abrir**.	open

Tabla 246. Acciones de usuario grabadas y mandatos de Selenium IDE (continuación)	
Acción de usuario	**Mandatos añadidos al script**
Para asegurarse de que el script comprueba que se carga la página web, pulse con el botón derecho del ratón en el texto del título de la página web (IBM Cloud Application Performance Management) y pulse **Mostrar todos los mandatos disponibles** > **verifyTitle IBM Cloud Application Performance Management**.	`verifyTitle`
Para registrar cuándo el usuario pulsa un enlace para ver detalles sobre Cloud APM, pulse el enlace **Detalles**. Se carga la página **Detalles**.	`clickAndWait`
Para asegurarse de que el script comprueba que la página **Details** se ha cargado, pulse con el botón derecho del ratón sobre la cabecera "Puntos destacados de característica" y seleccione **Mostrar todos los mandatos disponibles** > **verifyText css=h2.heading--TERTIARY**.	`verifyText`
Para registrar cuándo el usuario pulsa un enlace para ver detalles sobre cómo adquirir Cloud APM, pulse el enlace **Detalles**. Se cargará la página **Purchase**.	`clickandWait`
Para registrar cuando el usuario pulsa un botón para registrarse para una prueba gratuita de Cloud APM, pulse el botón **Try Free**.	`click`

2. En la ventana de Selenium IDE, pulse **Grabar** para detener la grabación. Pulse la herramienta **Guardar proyecto**, asigne un nombre significativo al script y guárdelo como archivo `.side` (por ejemplo, `open_webpage.side`).
3. En la ventana de Selenium IDE, revise el script grabado. Pulse la pestaña **Tabla** para mostrar el script en un formato de tabla. En la ventana de Selenium IDE, pulse **Play Current Test Case** para probar la reproducción del script grabado.

   En este ejemplo, Selenium IDE muestra el script de acciones de usuario en el sitio web IBM Marketplace, tal como se describe en el paso 1.

Tabla 247. Ejemplo de un script Selenium IDE que registra las acciones de usuario en el sitio web IBM Marketplace		
Mandato	**Destino**	**Valor**
`open`	`/`	
`verifyTitle`	`IBM Cloud Application Performance Management`	
`clickAndWait`	`css=ul > #details > a`	
`verifyText`	`css=h2.heading--TERTIARY`	Puntos destacados de la característica
`clickAndWait`	`css=ul > #purchase > a`	
`click`	`link=Try Free`	

Resultados

Habrá grabado un script que puede utilizar para supervisar el rendimiento y la disponibilidad de una aplicación web.

Qué hacer a continuación

Si ha grabado un script complejo, puede organizar el script en scripts más simples, donde cada script representa un proceso de negocio específico o una acción de usuario en la aplicación web.

Utilice el Gestor de scripts sintéticos para cargar su archivo de script en una transacción sintética nueva o existente.

Estructuración de scripts complejos
Organice un script complejo en varios scripts; a continuación, guarde los scripts juntos en una colección de scripts denominada *conjunto de pruebas*.

Acerca de esta tarea

Si crea un script complejo, puede organizar los script en scripts simples que representan distintos procesos de negocio o de usuario en la aplicación web. Guarde los scripts juntos como un conjunto de pruebas. Puede utilizar después estos scripts para supervisar el rendimiento y la disponibilidad de la aplicación web en respuesta a acciones de usuario específicas en el Panel de instrumentos del rendimiento de aplicaciones.

Debe haber sólo un conjunto de pruebas, al que deben añadirse todas las pruebas.

Importante: Se recomienda organizar scripts complejos en scripts individuales, donde cada script representa un proceso de negocio o de usuario típico que desea supervisar. Por ejemplo, cree scripts individuales que registran cuándo inicia sesión un usuario o busca un elemento en un sitio web. Si organiza los scripts de acuerdo con los procesos de usuario o de negocio, puede supervisar entonces la respuesta de la aplicación web a estos procesos específicos en el Panel de instrumentos del rendimiento de aplicaciones.

Procedimiento

Para organizar el script complejo en scripts individuales y guardar los scripts como un conjunto de pruebas, realice los pasos siguientes:

1. Para crear un script individual para cada proceso de usuario grabado en el script, pulse **Pruebas** > **+** en Selenium IDE. Asigne a cada script un nombre significativo que describa el proceso de usuario y guarde cada script como archivo `.side`, por ejemplo `load_homepage.side`.

   Para obtener más información, consulte "Grabación de scripts sintéticos" en la página 1062.

   Importante: El nombre proporcionado al script en Selenium IDE es el nombre que identifica el proceso de usuario o de negocio grabado que puede supervisar en el Panel de instrumentos del rendimiento de aplicaciones.
2. En Selenium IDE, abra un script complejo que ha grabado anteriormente. Organice los mandatos de script en scripts individuales, de acuerdo con distintas acciones de usuario. **Corte** mandatos del script complejo original en la ventana **Caso de prueba** y **Pegue** mandatos en los distintos scripts de la ventana **Caso de prueba**.

   Por ejemplo, el ejemplo de script complejo de Grabación de scripts sintéticos contiene mandatos de Selenium IDE para tres procesos de usuario distintos.

   - Abra la página de inicio de Cloud APM en el sitio web IBM Marketplace.
   - Abra la página **Detalles** en IBM Marketplace.
   - Abra la página **Pricing** y grabe cuándo el usuario abre la página de registro para una prueba gratuita.

   Las acciones de usuario se organizan después en tres tipos de script.

Tabla 248. Script de ejemplo para abrir la página de IBM Marketplace (`load_homepage.side`)

Mandato	Destino	Valor
`open`	`/`	
`verifyTitle`	`IBM Cloud Application Performance Management`	

*Tabla 249. Script de ejemplo para abrir la página **Details** en IBM Marketplace (load_products.side)*

Mandato	Destino	Valor
clickAndWait	css=ul > #details > a	
verifyText	css=h2.heading--TERTIARY	Puntos destacados de la característica

*Tabla 250. Script de ejemplo para abrir las páginas **Purchase** y de registro de prueba en IBM Marketplace (load_APM.side)*

Mandato	Destino	Valor
clickAndWait	css=ul > #purchase > a	
click	link=Try Free	

3. Para colocar casos de prueba individuales en un conjunto de pruebas, cambie a la ventana **Conjunto de pruebas** y añada pruebas al conjunto de pruebas de acuerdo con la secuencia de lógica empresarial. Por último, pulse la herramienta **Guardar proyecto** para guardar el conjunto de pruebas y todas las pruebas que contiene en un archivo `.side`.
   A modo de ejemplo, considere la secuencia lógica `Load_URL`, `Select Manage inventory`, `Select IBM Machine Type`. Al añadir estos casos de prueba al conjunto de pruebas, primero comprobaremos `Load_URL`, seguido de `Select Manage inventory`, y luego `Select IBM Machine Type`.

Resultados
Habrá grabado un conjunto de scripts que puede utilizar para supervisar el rendimiento y la disponibilidad de las aplicaciones web. Utilice el Gestor de scripts sintéticos para cargar el conjunto de pruebas de scripts `.side` en una transacción sintética nueva o existentes.

Actualización de scripts desde versiones anteriores de Selenium IDE
Las versiones 2.2.X y 3.2.X de Selenium IDE soportadas utilizan el formato `.side` para grabar scripts sintéticos en lugar del formato `.html` utilizado por las versiones anteriores de Selenium IDE. Si tiene scripts `.html` preexistentes, puede seguir utilizándolos. Es posible que los scripts creados con versiones anteriores de Selenium IDE no funcionen plenamente con los controladores más recientes de Firefox y Selenium utilizados por IBM Cloud Availability Monitoring. En algunos casos, es posible que desee editar los scripts `.html`, volver a grabarlos en el nuevo formato `.side` o importar el script `.html` y guardarlo en el formato `.side`.

Procedimiento

- Excepción: si desea interactuar con el elemento `Select2`, no utilice el mandato **`select`** (consulte https://github.com/SeleniumHQ/selenium-ide).
  El script antiguo es

```
<td>select</td>
<td>id=country</td>
<td>label=United States</td>
```

  Debe cambiarse por

```
<tr>
   <td>runScript</td>
   <td>window.scrollTo(0,810)</td>
   <td></td>
</tr>
<tr>
   <td>click</td>
   <td>id=select2-country-container</td>
   <td></td>
</tr>
```

```
<tr>
   <td>click</td>
   <td>xpath=(//ul[@id='select2-country-results']/li[text() = 'United States'])</td>
   <td></td>
</tr>
```

- Limitación: los scripts `.side` registrados con Selenium IDE 3.2.X o 3.3.X están soportados; el ubicador **`linkText`** no está soportado.

Gestión de transacciones sintéticas
Utilice el Gestor de scripts sintéticos para crear, configurar y suprimir transacciones sintéticas.

Para mostrar el Gestor de scripts sintéticos, pulse el icono **Configuración del sistema** y seleccione **Gestor de scripts sintéticos**. Para trabajar en el Gestor de scripts sintéticos, debe ser miembro de un rol que tenga permiso de vista para el **Gestor de scripts sintéticos** y la **Configuración de agente**. Para obtener más información, consulte “Roles y permisos” en la página 1036.

Puede ver datos sobre el uso de transacciones sintéticas para aplicaciones web públicas dirigidas al exterior durante el mes actual. Vea el número de instancias de reproducción realizadas e instancias de reproducción previstas según la configuración actual del mes actual en la tabla Uso de reproducción mensual del Gestor de scripts sintéticos.

Importante: Para crear transacciones sintéticas para aplicaciones web privadas internas y externas, debe instalar el Agente de Synthetic Playback en cada ubicación que contiene una aplicación web que desea supervisar.

Puede realizar las tareas siguientes con el Gestor de scripts sintéticos:

- Crear y editar una transacción sintética.
- Configurar las variables de transacción sintética.
- Suprimir una transacción sintética.

Creación y edición de transacciones sintéticas
Para ver datos sobre el rendimiento y la disponibilidad de una aplicación web, primero debe crear una transacción sintética en el Gestor de scripts sintéticos.

Acerca de esta tarea
Utilice el Gestor de scripts sintéticos para crear, editar y configurar una transacción sintética. Escriba el URL de una aplicación web en el Editor de scripts sintéticos para generar un script simple para la transacción sintética. Para simular procesos de usuario complejos, suba un script sintético en una transacción sintética en el Editor de scripts sintéticos. A continuación, configure la transacción sintética para que se ejecute a intervalos regulares y en distintas ubicaciones.

Procedimiento

Para crear una transacción o editar una transacción existente, realice los pasos siguientes:

1. Opcional: Si no se muestra el Gestor de scripts sintéticos, pulse el icono **Configuración del sistema** y seleccione **Gestor de scripts sintéticos**.
2. Para crear una nueva transacción, pulse el icono **Nuevo**. Para editar una transacción existente, pulse el icono **Editar**.
3. En el **Editor de scripts sintéticos**, pulse la pestaña **Cargar un script** y especifique un nombre de transacción en el recuadro de texto **Nombre de transacción**. Escriba una descripción de la transacción en el recuadro de texto **Descripción**.

   Importante: No ponga a la transacción el mismo nombre que una transacción que haya suprimido en las últimas 24 horas. Si pone a la transacción el mismo nombre que otra que ha suprimido recientemente, los datos de ambas transacciones se atribuyen incorrectamente a dicho nombre de transacción en Panel de instrumentos del rendimiento de aplicaciones.

4. Para generar un script simple para probar una aplicación web, seleccione **Especificar el URL de la página web a probar** y escriba un URL. El Gestor de scripts sintéticos genera un script sintético simple basado en dicho URL.
5. Para asignar un archivo de script creado anteriormente para la transacción, seleccione **Cargar archivo de script**. Pulse **Cargar script** para examinar los scripts del sistema. Elija un script y pulse **Abrir**.

   Importante: El archivo de script sintético debe ser uno de los tipos de archivo siguientes:

   - `.html`
   - `.zip`

   Guarde los scripts individuales simples (casos de prueba) como archivos `.html`. Comprima los casos de prueba y los conjuntos de prueba en un archivo `.zip`.
6. Para configurar la reproducción escalonada o simultánea de una transacción sintética, pulse la pestaña **Planificar un script**. Seleccione **Simultánea** para ejecutar la transacción de todas las ubicaciones simultáneamente, o seleccione **Escalonada** para ejecutar la transacción desde una ubicación diferente en cada intervalo.
7. Para elegir la frecuencia con la que se ejecuta un script, pulse la pestaña **Planificar un script**. Pulse el recuadro de texto **Intervalo** y especifique un número, basándose en la frecuencia con la que desea supervisar la aplicación web. Elija una longitud de intervalo entre `1` y `60` minutos.

   Nota: Los scripts largos o complejos pueden llevar más tiempo ejecutarse. Elija una longitud de intervalo más larga para scripts complejos o largos.
8. Para elegir las ubicaciones de reproducción del script, pulse la pestaña **Planificar un script** y, a continuación, seleccione las ubicaciones de centros de datos y las ubicaciones de instalación de agente donde desea que se ejecute el script.
9. Para establecer umbrales de tiempo de respuesta para las transacciones y subtransacciones sintéticas, pulse la pestaña **Configuración avanzada**; a continuación, pulse y expanda una transacción sintética para revelar todas las subtransacciones. Efectúe una doble pulsación en el valor de umbral de tiempo de respuesta y especifique un valor. Elija un valor entre `0` y `3600` segundos. Si no desea establecer un umbral, especifique `0`. El valor de umbral de tiempo de respuesta predeterminado es 10 segundos.

   Nota: Algunos mandatos pueden llevar más tiempo que otros. Elija un umbral de tiempo de respuesta que sea adecuado para el mandato que desea probar. Si la transacción prueba cuánto tiempo lleva abrir una página web, elija un tiempo de respuesta más largo.
10. Para acabar de crear o editar la transacción, pulse **Guardar**.

Resultados
Ha configurado una transacción sintética. La transacción sintética se enumera en el Gestor de scripts sintéticos.

Qué hacer a continuación
Puede ver las métricas y los ICR grabados por una transacción sintética en el Panel de instrumentos del rendimiento de aplicaciones. También puede añadir transacciones como componentes a una aplicación, y ver todas las transacciones sintéticas que están asociados con esa aplicación.

Importante: Cuando añade una transacción sintética por primera vez, puede aparecer un espacio en blanco en el widget de grupo **Disponibilidad a lo largo del tiempo** en Panel de instrumentos del rendimiento de aplicaciones. El espacio en blanco desaparece rápidamente cuando el servidor recibe el primer resultado de reproducción de la transacción.

Configuración de variables de transacciones sintéticas
Utilice el Gestor de scripts sintéticos para actualizar los valores de variables, como los nombres de usuario y las contraseñas almacenadas en scripts sintéticos, sin tener que editar los archivos de script. Los valores de las variables pueden ser exclusivos para cada ubicación de reproducción.Configure las variables para los scripts sintéticos cuando las aplicaciones web requieran valores de variable distintos

en ubicaciones distintas. Por ejemplo, si la aplicación web no permite los mismos detalles de inicio de sesión en ubicaciones distintas, utilice el Gestor de scripts sintéticos para proporcionar detalles de inicio de sesión distintos en cada ubicación. Puede crear variables en scripts sintéticos mediante el mandato `store` en el plug-in Selenium-IDE.

Acerca de esta tarea

En esta tarea, utilice el Gestor de scripts sintéticos para configurar las variables almacenadas en el script sintético.

Procedimiento

Para configurar las variables de una transacción sintética, realice los pasos siguientes:

1. Si no se muestra el Gestor de scripts sintéticos, pulse el icono **Configuración del sistema** y seleccione **Gestor de scripts sintéticos**. Seleccione una transacción sintética de la lista y pulse el icono **Editar**.
2. Seleccione las ubicaciones de reproducción para la transacción sintética.
3. Pulse la pestaña **Configuración avanzada**. Si el script sintético contiene variables, puede editar estas variables en la ventana **Configure las sustituciones de variables para ubicaciones diferentes**. Para editar una variable, efectúe una doble pulsación en el valor. Para finalizar, pulse **Guardar**.

   Por ejemplo, el script siguiente contiene las variables *nombre_usuario* y *contraseña*. Los valores de esas variables, `usuario1` y `pass`, se guardan mediante el mandato `store` en Selenium-IDE. Las variables tienen el mismo valor en dos ubicaciones, Dallas y San José.

   Tabla 251. Ejemplo de un script con variables

Mandato	**Destino**	**Valor**
`store`	`user1`	*nombreusuario*
`store`	`pass`	*contraseña*
`tipo`	`id=j_username`	*${username}*
`tipo`	`id=j_password`	*${password}*

   Los valores de las variables de script se muestran en la ventana **Configure las sustituciones de variables para ubicaciones diferentes**. Cambie el valor de *nombre_usuario* en la ubicación `Dallas` del `usuario1` por `admin1`, de modo que la transacción sintética utilice los detalles de inicio de sesión distintos en ubicaciones distintas.

   Tabla 252. Valores de variables de script en distintas ubicaciones

Ubicación	**username**	**contraseña**
San José	usuario1	pass
Dallas	admin1	pass

Resultados

Habrá configurado las variables de un transacción sintética. Puede utilizar ahora esta transacción sintética para probar el rendimiento y la disponibilidad de una aplicación web en ubicaciones distintas.

Qué hacer a continuación

Puede ver las métricas y los ICR grabados por una transacción sintética en el Panel de instrumentos del rendimiento de aplicaciones. También puede añadir transacciones como componentes a una aplicación, y ver todas las transacciones sintéticas que están asociados con esa aplicación.

Filtrar URLs y nombres de dominio para las transacciones sintéticas
Utilice el Gestor de scripts sintéticos para permitir o bloquear el acceso a URL y dominios específicos añadiendo reglas a la lista blanca y negra para la prueba.

Acerca de esta tarea

Puede controlar qué dependencias y recursos contribuyen a los tiempos de respuesta de las aplicaciones web probadas. Utilice la lista negra para filtrar peticiones de dominios especificados para eliminar dichas solicitudes de los tiempos de respuesta medidos. Utilice la lista blanca para incluir las peticiones de dominios especificados para añadir esas solicitudes a los tiempos de respuesta medidos. Utilice la lista negra y la lista blanca para filtrar o incluir dependencias que están asociadas con la aplicación web, como por ejemplo mediciones de terceros.

El campo **Lista negra** contiene una lista de reglas que bloquean el acceso a URLs y dominios especificados.

El campo **Lista blanca** contiene una lista de reglas que permiten el acceso a URLs y dominios especificados.

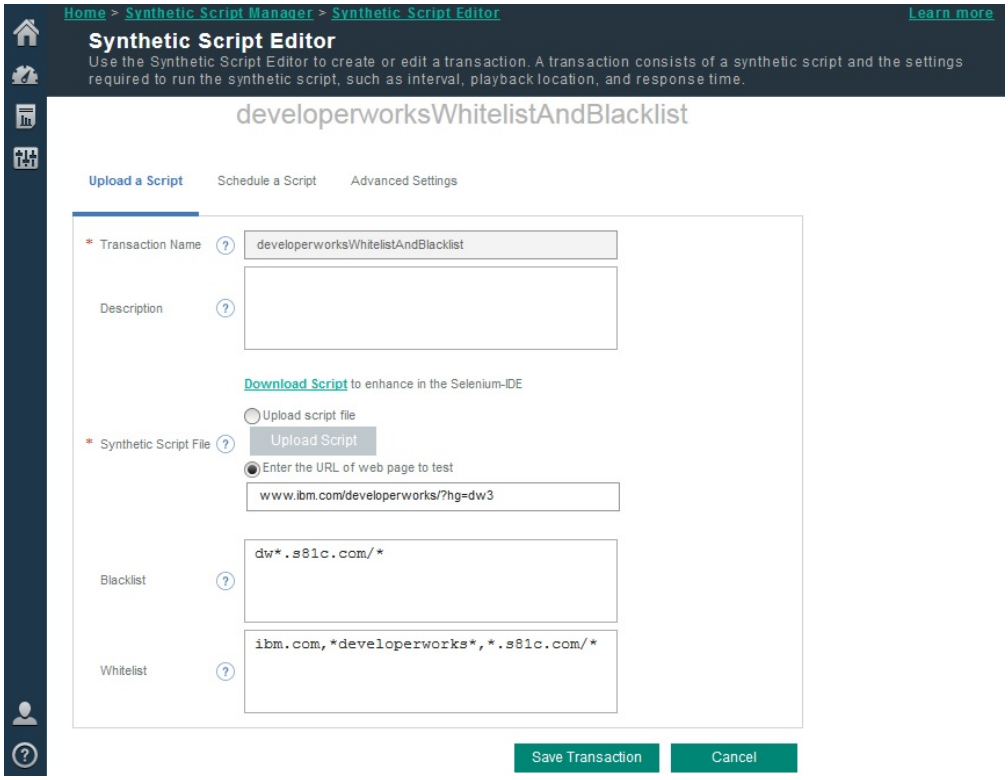
Utilice comas (,) para separar las reglas en la lista negra y blanca. Utilice el símbolo de comodín (*) para filtrar los nombres de dominio y los URL. Por ejemplo, `ibm.com, *.bluemix.net, *developerworks*, *.profile.*.cloundfront.net/*.png`.

Nota: si configura una lista negra y una lista blanca para la transacción sintética, la lista negra tiene mayor prioridad.

Procedimiento

Para añadir una regla a la lista negra o blanca de la transacción sintética, siga estos pasos:

1. Si no se muestra el Gestor de scripts sintéticos, pulse el icono **Configuración del sistema** y seleccione **Gestor de scripts sintéticos**.
2. Para configurar la lista negra o blanca para una transacción existente, pulse el icono **Editar**. Si no se listan transacciones, pulse el icono **Nuevo** para crear una transacción.
3. En el **Editor de scripts sintéticos**, pulse la pestaña **Cargar un script** y especifique un nombre de transacción en el recuadro de texto **Nombre de transacción**. Añada reglas a los recuadros de texto **Lista negra** y **Lista blanca**.



Resultados
Ahora, la transacción sintética filtrará las solicitudes no deseadas para la aplicación web y permitirá el acceso a otras solicitudes específicas.

Ocultación de contraseñas en el Gestor de scripts sintéticos
Almacene contraseñas como variables en los scripts sintéticos para ocultar valores de contraseñas en el Gestor de scripts sintéticos.

Antes de empezar
Este procedimiento requiere que edite un script sintético. Registre un script sintético mediante Selenium IDE. Para obtener más información, consulte "Grabación de scripts sintéticos" en la página 1062.

Acerca de esta tarea

Modifique manualmente los scripts sintéticos de Selenium IDE para almacenar la contraseña como una variable. A continuación, cree transacciones sintéticas con contraseñas ocultas en el Gestor de scripts sintéticos. Las contraseñas ocultas se visualizan como asteriscos en el Gestor de scripts sintéticos.

Importante: Se recomienda que almacene las contraseñas en scripts sintéticos para que los valores de contraseña no se visualicen en el Gestor de scripts sintéticos. Las contraseñas ocultan hacen que las aplicaciones web sean más seguras, ya que evita que otras personas visualicen las contraseñas.

Procedimiento

1. Abra el script que desee modificar en Selenium IDE. Utilice el mandato `store` para asignar una contraseña a la variable *password*, siguiendo el ejemplo que se describe en este paso y, a continuación, guarde el script.

   Importante: Debe almacenar la contraseña como el nombre de variable *password*, ya que la contraseña no se visualiza en el Gestor de scripts sintéticos.

Por ejemplo, el siguiente script sintético contiene un nombre de usuario *test@example.com* y un valor de contraseña *ibm4value*.

```
<tr>
   <td>type</td>
   <td>id=username</td>
   <td>test@example.com</td>
</tr>
<tr>
   <td>type</td>
   <td>id=password</td>
   <td>ibm4value</td>
</tr>
```

El script siguiente muestra cómo asignar el valor de contraseña *ibm4value* a la variable *password* mediante el mandato `store`.

```
<tr>
   <td>store</td>
   <td>ibm4value</td>
   <td>password</td>
</tr>
<tr>
   <td>type</td>
   <td>id=username</td>
   <td>test@example.com</td>
</tr>
<tr>
   <td>type</td>
   <td>id=password</td>
   <td>$(password)</td>
</tr>
```

2. Opcional: Para ocultar la contraseña a nivel de script, asigne un valor en blanco a la variable *password* mediante el mandato `store` y, a continuación, guarde el script.

   Puede establecer la contraseña posteriormente en el Gestor de scripts sintéticos.

   Por ejemplo, el script siguiente muestra cómo asignar un valor en blanco a la variable *password* mediante el mandato `store`.

```
<tr>
   <td>store</td>
   <td></td>
   <td>password</td>
</tr>
<tr>
   <td>type</td>
   <td>id=username</td>
   <td>test@example.com</td>
</tr>
<tr>
   <td>type</td>
   <td>id=password</td>
   <td>$(password)</td>
</tr>
```

3. Inicie sesión en la Consola de Cloud APM y abra el **Gestor de scripts sintéticos**. Cree una transacción y cargue el script a dicha transacción. Pulse la pestaña **Configuración avanzada**.

   La contraseña de cada una de las ubicaciones está oculta. Puede cambiar la contraseña de cada una de las ubicaciones. Para obtener más información, consulte "Gestión de transacciones sintéticas" en la página 1067.

Supresión de una transacción sintética

Utilice el Gestor de scripts sintéticos para suprimir las transacciones sintéticas.

Procedimiento

Para suprimir una transacción sintética, realice los pasos siguientes:

1. Si se asigna una transacción sintética a una aplicación, debe eliminar primero la transacción de esa aplicación. En Panel de instrumentos del rendimiento de aplicaciones, pulse y expanda **Todas mis**

aplicaciones y, a continuación, pulse la aplicación asociada a la transacción sintética que desea suprimir. Pulse el icono **Editar** . En la ventana **Editar aplicación**, elimine el componente de transacción sintética de la aplicación. Para obtener más información, consulte Gestión de aplicaciones.

Ahora se puede suprimir la transacción sintética.

2. En la barra de navegación, pulse el icono **Configuración del sistema** y seleccione **Gestor de scripts sintéticos**. Seleccione una transacción sintética y luego pulse el icono **Suprimir** . Para confirmar que desea suprimir esta transacción sintética, pulse **Aceptar**.

Resultados
Se suprimirá la transacción sintética.

Visualización de datos de transacciones sintéticas en el Panel de instrumentos del rendimiento de aplicaciones

Vea datos de transacciones sintéticas en Panel de instrumentos del rendimiento de aplicaciones. Asocie transacciones sintéticas con una aplicación nueva o existente y vea todas las transacciones sintéticas asociadas juntas en Panel de instrumentos del rendimiento de aplicaciones.

Acerca de esta tarea

Puede ver los datos de transacciones sintéticas en la ventana **Mis transacciones** en Panel de instrumentos del rendimiento de aplicaciones.

También puede crear grupos de transacciones sintéticas asociando sus transacciones con una aplicación. Utilice la herramienta **Añadir aplicación** o **Editar aplicación** en Panel de instrumentos del rendimiento de aplicaciones para añadir transacciones sintéticas como componentes a una aplicación web nueva o existente. A continuación, puede ver datos de todas las transacciones sintéticas que están asociadas con dicha aplicación juntos en Panel de instrumentos del rendimiento de aplicaciones.

Si ya utiliza el agente de tiempo de respuesta para supervisar el tiempo de respuesta del usuario para una aplicación, puede añadir una transacción sintética a esa transacción. A continuación, puede ver más métricas e ICR para esa aplicación en el Panel de instrumentos del rendimiento de aplicaciones.

Procedimiento

- Para ver transacciones sintéticas, complete el paso siguiente:
  a) Pulse el icono **Rendimiento** y seleccione **Panel de instrumentos del rendimiento de aplicaciones**. En la ventana **Aplicaciones**, expanda **Todas mis aplicaciones** y seleccione **Mis transacciones**. En la ventana **Grupos**, expanda **Transacciones** y seleccione **Transacciones sintéticas**.
  b) Pulse una transacción sintética para ver la disponibilidad y los datos de rendimiento de esa transacción, junto con un gráfico de tiempos de respuesta de las instancias de transacción durante un periodo definido.
- Para asociar transacciones sintéticas a una aplicación, complete los pasos siguientes:
  a) Pulse el icono **Rendimiento** y seleccione **Panel de instrumentos del rendimiento de aplicaciones**. Seleccione y edite una aplicación existente o cree una aplicación nueva. Para obtener más información, consulte Gestión de aplicaciones.
  b) En la ventana **Añadir aplicación**, pulse el icono **Añadir componentes** y seleccione **Transacciones sintéticas** en la lista de componentes. En la ventana **Editor de componentes**, seleccione una transacción sintética y pulse **Añadir** para asociar la transacción sintética a la aplicación.
  c) Pulse **Atrás**. Pulse **Cerrar** para cerrar la ventana **Editor de componentes**. Pulse **Guardar**. Para añadir otra transacción sintética como un componente, repita los pasos 1 a 3.

Resultados
Habrá asociado una transacción sintética a una aplicación. Ahora puede ver la aplicación y sus transacciones sintéticas asociadas en Panel de instrumentos del rendimiento de aplicaciones. Para obtener más información, consulte Gestión de aplicaciones.

Nota: Cuando asocia una transacción sintética a una aplicación, la disponibilidad inicial de esa aplicación es desconocida. Puede llevar varios minutos actualizarse el estado.

Gestión de sucesos sintéticos
Utilice el gestor de umbrales y el gestor de grupos de recursos para configurar los umbrales y asignarlos a las transacciones sintéticas. Se generan los sucesos sintéticos cuando el valor de un atributo de transacción coincide con el definido en el umbral. Puede supervisar sucesos sintéticos en Panel de instrumentos del rendimiento de aplicaciones.

Creación de un umbral para transacciones sintéticas
Utilice el Gestor de umbrales para crear umbrales para las transacciones sintéticas. Los umbrales se utilizan para comparar los valores de atributo con los valores establecidos en el umbral. Si el valor muestreado satisface la comparación, se genera un suceso.

Acerca de esta tarea

Los umbrales permiten a los usuarios supervisar el momento en que las aplicaciones notifican condiciones específicas. Por ejemplo, puede crear un umbral para supervisar el tiempo que lleva a un sitio web responder a un mandato de usuario en particular. Si al sitio web le lleva más tiempo del tiempo especificado en el umbral, se genera un suceso sintético.

Procedimiento

Para crear un umbral y asociarlo a una o varias transacciones sintéticas, complete los pasos siguientes:

1. En la barra de navegación, pulse el icono **Configuración del sistema** y seleccione **Gestor de umbrales**. Establezca el tipo de **Origen de datos** como **Transacción sintética**.
2. Cree un umbral. Para obtener más información, consulte “Gestor de umbrales” en la página 1019.
3. Para asociar el umbral a una transacción, seleccione **KSO TRANSACTION** como el **Conjunto de datos** y luego seleccione **TRANSNAME** como el **Elemento de visualización**. Para el **Operador lógico**, seleccione **And (&)**.

   Nota: Debe seleccionar **TRANSNAME** como el **Elemento de visualización**. Si no selecciona **TRANSNAME**, no podrá ver los sucesos sintéticos en el Application Performance Dashboard.
4. Para añadir una condición, pulse el icono **Nueva condición**. En el recuadro Nueva condición, seleccione un **Atributo** y un **Operador**. A continuación, introduzca un valor de umbral para **Valor**. Para añadir esta condición al umbral, pulse **Aceptar**.

   Por ejemplo, para añadir una condición de umbral que genera un suceso sintético cuando más del 50 % de las transacciones son lentas, seleccione **PSLOW** como **Atributo** y luego seleccione **Mayor que** como **Operador**. Para establecer el porcentaje de transacciones lentas para generar el suceso, introduzca 50 como el **Valor**.
5. Para definir más atributos de umbral, añada más condiciones al umbral.
6. Cuando haya terminado, pulse **Guardar**. Si no desea asignar el umbral a un grupo de recursos, pulse **Aceptar**.

Resultados
Habrá creado un umbral y lo habrá asociado a una transacción sintética. Cuando se cumplen las condiciones de umbral, se genera un suceso. Puede supervisar los sucesos en Panel de instrumentos del rendimiento de aplicaciones, de la pestaña **Sucesos**.

Qué hacer a continuación
Puede agrupar las transacciones sintéticas en grupos de recursos.

Creación de un grupo de recursos para transacciones sintéticas

Organice las transacciones sintéticas en un grupo de recursos y aplique umbrales a todas las transacciones en ese grupo de recursos.

Antes de empezar

Cree un umbral que se aplica a todas las transacciones sintéticas en su grupo de recursos.

Acerca de esta tarea

Puede organizar las transacciones sintéticas en grupos de recursos y aplicar umbrales a cada transacción sintética en ese grupo de recursos. Utilice el gestor de grupos de recursos para crear un grupo de recursos y asigne un umbral a ese grupo de recursos. A continuación, asigne uno o varios subnodos de transacciones sintéticas a ese grupo de recursos. El umbral que está asociado con el grupo de recursos ahora se aplica a todas las transacciones sintéticas asociadas.

Procedimiento

Para crear un grupo de recursos para transacciones sintéticas, complete los pasos siguientes:

1. Pulse el icono **Configuración del sistema** y seleccione **Gestor de grupos de recursos**. Cree un grupo de recursos o edite un grupo de recursos existente. Para obtener más información, consulte "Gestor de grupos de recursos" en la página 1014.

Para crear un grupo de recursos para transacciones sintéticas, complete los pasos siguientes:

2. Proporcione al grupo de recursos un nombre y una descripción. Asigne un umbral al grupo de recursos en la tabla **Asignación de umbral** y pulse **Guardar**. En el Gestor de grupos de recursos, seleccione el grupo de recursos de nuevo y pulse el icono **Editar** .
3. Asocie el grupo de recursos con los subnodos de transacción sintética de la tabla **Asignación de recursos** y pulse **Guardar**.

   El formato de subnodos de transacción sintética es S0:*NombreTransacción*. Por ejemplo, si tiene una transacción open_webpage, el subnodo disponible se denomina S0:open_webpage.

Resultados

Ha organizado las transacciones sintéticas en un grupo de recursos, y ha aplicado un umbral a cada transacción en ese grupo de recursos.

Creación de umbrales críticos para transacciones sintéticas simultáneas y escalonadas

Utilice el Gestor de umbrales para crear umbrales críticos para transacciones sintéticas simultáneas y escalonadas.

Acerca de esta tarea

Cree umbrales que notifiquen a las partes interesadas cuando fallan transacciones escalonadas consecutivas o cuando fallan transacciones simultáneas en todas las ubicaciones de reproducción. Para obtener más información, consulte "Creación y edición de transacciones sintéticas" en la página 1067.

Procedimiento

Para crear un umbral crítico que crea un suceso cuando fallan las instancias de reproducción de transacciones escalonadas, complete los pasos siguientes:

1. Cree un umbral para transacciones sintéticas en el Gestor de umbrales. Para obtener más información, consulte "Creación de un umbral para transacciones sintéticas" en la página 1074.
2. En el Gestor de umbrales, seleccione **Crítico** como **Gravedad** y entre 1 minuto como **Intervalo (HHMMSS)** de umbral. Utilice la fórmula siguiente para determinar las **Muestras consecutivas obligatorias**:

   Muestras consecutivas obligatorias = (intervalo reproducción * errores consecutivos esperados) - 1

Por ejemplo, si el intervalo de reproducción de la transacción sintética que desea supervisar es 5 minutos y desea detectar 8 errores de reproducción consecutivos, debe establecer **Muestras consecutivas obligatorias** como (5 * 8) - 1 = 39.

3. Añada una condición. En el cuadro Nueva condición, seleccione **LOCATION** como **Atributo**, seleccione **Igual a** como **Operador** y entre `Ninguno` como **Valor**. Añada una segunda condición y establezca **PFAILED** = `100`. Guarde el umbral.
4. En la barra de navegación, abra el **Gestor de grupos de recursos**. Cree un grupo de recursos. Asigne una o más transacciones sintéticas escalonadas al grupo de recursos y, a continuación, asigne el umbral que ha creado en los pasos 1-3 al grupo de recursos. Guarde el grupo de recursos. Para obtener más información, consulte "Creación de un grupo de recursos para transacciones sintéticas" en la página 1075.

Para crear un umbral crítico que crea un suceso cuando fallan las instancias de reproducción de transacciones simultáneas en varias ubicaciones, complete los pasos siguientes:

5. Cree un umbral para transacciones sintéticas en el Gestor de umbrales. Para obtener más información, consulte "Creación de un umbral para transacciones sintéticas" en la página 1074.
6. En el Gestor de umbrales, seleccione **Crítico** como **Gravedad** y entre 1 minuto como **Intervalo (HHMMSS)**. Establezca las **Muestras consecutivas obligatorias** como el mismo valor que el intervalo de reproducción de la transacción que desea supervisar.

   Por ejemplo, si el intervalo de reproducción de la transacción sintética que desea supervisar es 5 minutos, establezca **Muestras consecutivas obligatorias** en 5.
7. Añada una condición. En el cuadro Nueva condición, seleccione **LOCATION** como **Atributo**, seleccione **Igual a** como **Operador** y entre `Ninguno` como **Valor**. Añada una segunda condición y establezca **PFAILED** = `100`. Guarde el umbral.
8. Cree un grupo de recursos. Asigne una o más transacciones sintéticas y el nuevo umbral crítico a su grupo de recursos. Para obtener más información, consulte "Creación de un grupo de recursos para transacciones sintéticas" en la página 1075.

Resultados

Ha creado un umbral crítico para una transacción sintética escalonada o simultánea. Cuando se cumplen las condiciones de umbral, se genera un suceso. Puede supervisar los sucesos en Panel de instrumentos del rendimiento de aplicaciones, de la pestaña **Sucesos**.

Gestión de notificaciones de correo electrónico para los sucesos sintéticos

Utilice el Gestor de grupos de recursos e IBM Alert Notification para generar las notificaciones de correo electrónico cuando el rendimiento de la aplicación supera los umbrales.

Antes de empezar

Para configurar las notificaciones de correo electrónico para los sucesos sintéticos, debe habilitar primero Alert Notification para la suscripción. Para obtener más información, consulte Notificaciones de alertas en IBM Knowledge Center.

Acerca de esta tarea

En el Gestor de grupos de recursos, consulte Alert Notification para configurar las notificaciones de correo electrónico. Las notificaciones de correo electrónico se generan cuando el rendimiento de las aplicaciones cumple las condiciones establecidas por los umbrales asociados al grupo de recursos.

Procedimiento

Para gestionar las notificaciones por correo electrónico, siga estos pasos:

1. Pulse el icono **Configuración del sistema** y seleccione **Gestor de grupos de recursos**. Cree o edite un grupo de recursos.
2. Seleccione un umbral en la tabla **Asignación de umbral** y pulse **Guardar**. A continuación, asocie su grupo de recursos con un recurso Reproducción sintética o un recurso de agente Sucesos sintéticos en

la tabla **Asignación de recursos**. Pulse **Guardar**. En el Gestor de grupos de recursos, seleccione el grupo de recursos de nuevo y pulse el icono **Editar** .

3. Para iniciar Alert Notification en una pestaña nueva, pulse **Configurar notificación de correo electrónico** en el Gestor de grupos de recursos. En Notificación de alertas, pulse **Usuarios** en la barra de navegación para crear o editar los destinatarios de notificaciones de correo electrónico. Para obtener más información, consulte Notificaciones de alertas en IBM Knowledge Center.
4. En Alert Notification, pulse **Políticas de notificación** en la barra de navegación. Se proporcionará automáticamente al **Editor de notificaciones** una nueva política. El nombre y el filtro se derivan del grupo de recursos. Pulse **Añadir regla** para definir las condiciones que determinan cuándo se envía una notificación de correo electrónico. Para obtener más información, consulte Notificaciones de alertas en IBM Knowledge Center.
5. Para acabar de configurar las notificaciones de correo electrónico, pulse **Guardar**. La política se enumera en una tabla de la pestaña **Políticas de notificación**.

Directrices para maximizar el rendimiento de agente y servidor para la supervisión de archivos de registro

Para asegurarse de obtener el máximo rendimiento de los agentes de sistema operativo y el servidor Performance Management, debe definir las expresiones regulares en el archivo de formato (.fmt) y limitar también el número de sucesos de supervisión de archivos de registro que se notifican a la Consola de Cloud APM.

Directrices para definir expresiones regulares en el archivo `.fmt`

El archivo `.fmt` utiliza expresiones regulares que requieren una gran cantidad de proceso de CPU. Para mejorar el rendimiento del agente y servidor, minimice el tiempo invertido en comprobar registros en la supervisión del registro de origen en la expresión regular en el archivo `.fmt` utilizando las directrices siguientes:

Minimice el uso de los patrones de varias líneas.

Los patrones de varias líneas son caros porque el agente debe determinar cuáles son los registros y si coinciden. Cuando se utiliza un patrón de varias líneas que es una expresión regular que contiene el carácter "\n" o un formato de estilo TEC que contiene el símbolo '%n', el agente debe desglosar primero el archivo supervisado en registros de varios tamaños. A continuación, el agente debe comprobar los registros con respecto a las expresiones en el archivo de formato. Este procedimiento requiere que se comprueben dos veces las expresiones regulares, por lo que el proceso es lento. Si utiliza el patrón de una sola línea, se supone que cada línea del archivo es un registro y el proceso es mucho más rápido.

En algunos casos, podría ser posible ignorar algunas de las líneas y conseguir un mejor rendimiento. Por ejemplo, aquí se muestra un único registro de un registro de rastreo RAS1:

```
(4D66DACB.0001-1:RAS1,400,"CTBLD")
```

```
+4D66DACB.0001 Component: ira
```

```
+4D66DACB.0001 Driver: agent_fac:15/4114877.7
```

```
+4D66DACB.0001 Timestamp: Feb 24 2011 13:18:54
```

```
+4D66DACB.0001 Target: sos510amdx6-d
```

En el ejemplo, si solo está interesado en procesar esta línea:

```
+4D66DACB.0001 Driver: agent_fac:15/4114877.7
```

puede escribir el patrón de línea única siguiente:

```
^\+.*Driver: agent_fac:([0-9\.\/]+)$
```

Este patrón de una sola línea procesa el valor importante que necesita sin requerir el formato de varias líneas. Las otras cuatro líneas del registro lógico se tratan como registros de una sola línea que no coinciden con nada y se descartan.

Ordene las expresiones del archivo de formato por frecuencia de aparición en el registro de supervisión.

El agente comprueba cada registro que lee del registro con respecto a las expresiones en el archivo de formato, hasta que encuentra una coincidencia. Se inicia con la expresión final del archivo, y busca hacia arriba. Cuando se encuentra una coincidencia, la búsqueda se detiene. Si la expresión registrada más habitualmente se lista en último lugar, cuando se registra dicha expresión es la única expresión que se comprueba.

Si tiene 100 expresiones en el archivo de formato, cada vez que un registro de anotaciones coincide con el primero que aparece listado en el archivo de formato, en primer lugar, el agente debe comprobar las otras 99 expresiones, lo que ralentiza el proceso. Cuando un registro leído del registro no coincide con ninguno de los patrones del archivo de formato, el agente debe comprobarlo primero respecto a todos los patrones para saber si no coincide. Este proceso es lento y costoso.

Incluya la mayor cantidad de datos constantes posible en la expresiones regulares.

Por ejemplo, si se devuelve el siguiente error en el registro:

```
Error
de disco en el dispositivo: /dev/sda1 Error de disco en el
dispositivo: /dev/sdb2 yyy
```

puede escribir la expresión:

```
^Disk.*: .*$
```

Esta expresión provoca una coincidencia, pero fuerza al motor de expresiones regulares a considerar más posibilidades en otras líneas que podrían ser similares pero que, al final, no coinciden, por ejemplo, si faltan dos puntos.

La expresión siguiente es más útil porque es más precisa y provoca que el motor de expresiones regulares deje de procesar errores que no coinciden:

```

^Disk error on device: /dev/sd[a-b][0-9]$
```

No utilice subexpresiones que no necesite.

Las subexpresiones que se muestran entre paréntesis en el ejemplo que sigue se utilizan para informar al motor de expresiones regulares que desea que utilice un valor devuelto en los datos comparados. Estas subexpresiones causan proceso adicional y no son necesarias si no se utiliza el valor devuelto. Por ejemplo, cuando se devuelve el error siguiente en el registro:

```
write failure in writing to client 9.27.135.191. Error Broken pipe
```

si incluye la expresión regular siguiente en el archivo de formato, el mensaje de error se captura al final; pero, si no utiliza el valor devuelto, el rendimiento se ve afectado negativamente.

```
REGEX
WriteFailure

^write failure in writing to client (.*)\. Error
(.*)$

ClientAddr $1
CustomSlot1

END
```

Utilice paréntesis en expresiones para fines de agrupación.

Puede utilizar el operador ? para informar al motor regex que no capture el valor devuelto. Por lo tanto, puede utilizar el operador ? para agrupar solo los valores que se han devuelto. Esta agrupación

tiene un impacto positivo en el rendimiento. Por ejemplo, si se devuelven los siguientes datos de rastreo:

```
Login succeeded on the first attempt for user Bob.
Login succeeded on the third attempt for user Joe.
```

Para encontrar coincidencias entre ambos valores devueltos, debe considerar el primer o tercer intento de inicio de sesión. Si no le importa qué intento de inicio de sesión específico se ha realizado correctamente o qué usuario específico ha tenido éxito, puede incluir esta expresión para agrupar los valores devueltos:

```
REGEX
LoginSuceeded

^login succeeded on the (?:[a-z]+) attempt for user ([A-Z][a-z]*)\.$

UserName $1
CustomSlot1
END
```

Si es posible, no utilice el operador OR (|) en las expresiones.

El operador | es costoso de procesar. El operador | provoca que el motor de expresiones regulares complete una copia de seguridad e intente encontrar coincidencias de valores inicialmente no coincidían. Este procedimiento es mucho más ineficiente que si se tienen dos expresiones individuales. Por ejemplo, si tiene la siguiente expresión:

```
REGEX DiskError
^.*disk error.*4|^.*disk failure.*4
END
```

es mucho más eficiente utilizar estas dos expresiones:

```
REGEX DiskError
^.*disk error.*4
END

REGEX DiskError
^.*disk failure.*4
END
```

Estas expresiones devuelven los mismos resultados.

Importante: Estas expresiones infringen la directriz para utilizar tantos datos constantes como sean posibles y demuestran solo los problemas con el operador |.

No utilice expresiones ambiguas.

Las expresiones ambiguos fuerzan al motor de expresiones regulares a hacer una copia de seguridad y buscar distintas formas de comparar una expresión. Para obtener más información, consulte Consejos sobre el rendimiento.

Podrían producirse expresiones ambiguas como resultado de una expresión incluida para desglosar un registro largo en muchas subexpresiones. En esta versión degenerada de este problema, la expresión tiene un espacio entre los dos (.*):

```
(.*) (.*)
```

En este ejemplo de la versión degenerada, el motor regex busca dos cadenas de expresiones separadas por un espacio. Sin embargo, * también coincide con un espacio, por lo que el motor regex podría asignar el primer espacio al que llegue inicialmente al primer (.*). Si llega al final del registro de entrada sin encontrar otro espacio, debe hacer una copia de seguridad y volver a intentarlo utilizando el espacio como el espacio literal llamado en la expresión.

Para mejorar el rendimiento, utilice solo expresiones específicas. Puede utilizar la herramienta Regex Pal para comprobar si el archivo de formato que define coincide con el registro de supervisión. Para obtener más información, consulte Regex Pal.

Directrices para limitar los sucesos de archivo de registro que se han notificado.

Las directrices siguientes limitan los sucesos de archivo de registro que podrían causar que los agentes de sistema operativo o el Servidor de Cloud APM tuvieran un bajo rendimiento:

Escriba formatos específicos en el archivo `.fmt`.
Escriba formatos en el archivo `.fmt` que sean específicos y devuelvan registros relevantes. Por ejemplo, puede generar un suceso para un error específico, por ejemplo, las líneas que empiezan con `Error:`, e ignorar las líneas que empiecen con `Warning:`

```
Error:  disk failure
Error: out of memory
WARNING: incorrect login
```

No active el valor Unmatchlog en el archivo `.conf`.
Asegúrese de que no activa el valor **Unmatchlog** en el archivo `.conf`, ya que este valor registra todos los archivos no coincidentes y sobrecarga el sistema de archivos.

Especifique la clase de suceso `*DISCARD*` en el archivo `.fmt`.
Intente limitar el uso de CPU del agente especificando la clase de suceso `*DISCARD*` predefinida en el archivo `.fmt` para descartar datos intencionadamente. Cuando se utiliza la clase de suceso `*DISCARD*`, no se crearán sucesos para los registros que coincidan con el patrón en el archivo `.fmt`. Por ejemplo:

```
REGEX *DISCARD*
```

Active la detección de sucesos duplicados durante un periodo de tiempo más amplio.
Puede activar la detección de sucesos duplicados utilizando las teclas siguientes en el archivo `.conf`:

- DupDetectionKeyAttributes
- EventSummaryInterval
- EventFloodThreshold

En este ejemplo, las líneas duplicadas se reconocen por los valores *msg* y *CustomSlot1*:

```
DupDetectionKeyAttributes=msg,CustomSlot1
EventSummaryInterval=300
EventFloodThreshold=send_first
```

Si tiene muchos sucesos duplicados, aplique los valores de umbral *send_first* o *send_none* a los sucesos. Para obtener más información, consulte “Detección y filtrado de sucesos duplicados” en la página 1052.

Escriba condiciones de umbral específicas.
Escriba condiciones de umbral específicas que limiten el conjunto de filas que coincidan con el umbral. Por ejemplo, la siguiente fórmula de umbral hace que se active el umbral sólo cuando un suceso de la clase de suceso FileSystemUsage tiene un valor superior o igual a 95 en CustomInteger1:

```
( Class == 'FileSystemUsage' AND CustomInteger1 >= 95)
```

Proporcione el conjunto correcto de archivos `.conf` y `.fmt` para el agente.
Asegúrese de proporcionar el conjunto correcto de archivos `.conf` y `.fmt` para el agente. Por ejemplo, si está configurando la supervisión de archivos de registro para el agente de sistema operativo Windows, asegúrese de que configura los archivos `.conf` y `.fmt` creados específicamente para el agente de sistema operativo de Windows.

Consulte la base de datos de alarmas de MongoDB para determinar el número de sucesos abiertos o la tasa de suceso.

- Complete los pasos siguientes para consultar la base de datos de alarmas de MongoDB para determinar el número de sucesos abiertos o la tasa de sucesos:

  1. Cree un archivo `event-query.js` con una consulta MongoDB para la base de datos de alarmas, por ejemplo:

– Esta consulta cuenta todos los sucesos abiertos y cerrados con el nombre de umbral siguiente:

```
UDB_DB_Pool_Hit_Rat_Pct_Crit_2 db.alarms.count
```

```
({"threshold_name" : "UDB_DB_Pool_Hit_Rat_Pct_Crit_2"})
```

– Esta consulta cuenta sucesos abiertos y cerrados en MongoDB:

```
db.alarms.count()
```

2. Ejecute este mandato para obtener los resultados de la consulta en el archivo `event-query.js`: **`/opt/ibm/mongodb/bin/mongo 127.0.0.1:27000/alarm -u user -p mongoUsrpasswd@08 <event-count.js`**.

- Limite la cantidad de CPU que especifique para la supervisión de registros. Para obtener más información, consulte “Variables de entorno de supervisión del archivo de registro” en la página 660.

Availability Monitoring

Con IBM Cloud Availability Monitoring, puede crear, editar, ver y suprimir las pruebas sintéticas que imitan el comportamiento de usuario final en las aplicaciones web.

El panel de instrumentos de Availability Monitoring muestra información de disponibilidad y tiempo de respuesta de las aplicaciones supervisadas, URL y API REST. Utilice el panel de instrumentos para supervisar alertas y actividades que están asociadas con la aplicación, URL o API REST en diferentes ubicaciones mediante gráficos, tablas de desglose y vistas de correlación.

Availability Monitoring está disponible para usuarios de la oferta de IBM Cloud Application Performance Management, Advanced on Cloud con el complemento Availability Monitoring.

Acerca de Availability Monitoring

Utilice Availability Monitoring para crear pruebas sintéticas que supervisan la disponibilidad y el rendimiento de las aplicaciones web de diferentes ubicaciones públicas y privadas a todas horas.

Cree pruebas con Availability Monitoring. Configure las pruebas para que se ejecuten a intervalos definidos y en ubicaciones seleccionadas. Descargue y despliegue sus propios puntos de presencia (PoP) personalizados en servidores locales o privados. Ejecute pruebas desde 15 PoP públicos en las siguientes ubicaciones:

Asia
Chennai, Hong Kong, Singapur y Tokio

Australia
Melbourne

Europa
Amsterdam, Frankfurt, Londres y París.

Centroamérica
México

Norteamérica
Dallas, San José, Toronto y Washington D.C.

Sudamérica
Sao Paulo

Cuando haya creado y configurado las pruebas, podrá ver los datos de disponibilidad y rendimiento para las aplicaciones en el panel de instrumentos de Availability Monitoring.

Availability Monitoring tiene las siguientes características clave:

Puede empezar a trabajar en menos de 5 minutos
Cree fácilmente pruebas de acción única para supervisar el rendimiento y la disponibilidad de la aplicación web en unos minutos.

Maximizar el tiempo de funcionamiento y el nivel de satisfacción del usuario
Supervise el tiempo de actividad y respuesta de las aplicaciones con frecuencia desde varias ubicaciones geográficas. Ejecute pruebas sintéticas para medir el rendimiento de carga de sitios web y llamadas de API. Supervise los scripts de Selenium que utiliza para imitar flujos de usuarios en diferentes ubicaciones.

Proactividad
Reciba notificaciones para avisarle de los problemas antes de que afecten a los usuarios. Puede utilizar el servicio de Alert Notification integrado para crear políticas de alerta que reduzcan el ruido de la alerta.

Identificar los motivos de error con rapidez y precisión
El análisis en cascada ayuda a identificar el paso exacto en el que se ha producido una anomalía y la razón de la misma; por ejemplo, enlaces rotos, imágenes sobredimensionadas, búsquedas lentas o solicitudes externas. Se crean automáticamente capturas de pantalla para ayudarle a diagnosticar errores del navegador y problemas de rendimiento histórico. Descargue informes de disponibilidad mensual, semanal y diaria y promedios de tiempo de respuesta para las pruebas.

Para trabajar en Availability Monitoring, debe ser miembro de un rol que tenga permiso de visualización para la aplicación que desea supervisar. Para obtener más información, consulte “Roles y permisos” en la página 1036.

Acceso a Availability Monitoring

La pestaña **Visión general de estado** de Availability Monitoring de la aplicación muestra información de resumen acerca de la disponibilidad y el estado de las pruebas.. Puede acceder al panel de instrumentos de Availability Monitoring desde la pestaña **Visión general de estado** de Availability Monitoring.

Acerca de esta tarea

Acceda a la página de resumen de Availability Monitoring pulsando una aplicación elegible en el panel **Todas mis aplicaciones** en el Panel de instrumentos del rendimiento de aplicaciones. Desde la página de resumen, puede añadir pruebas para su aplicación, ver pruebas existentes de la aplicación y ver el panel de instrumentos de Availability Monitoring.

Procedimiento

Para acceder a Availability Monitoring, realice los pasos siguientes:

1. Pulse el icono **Rendimiento**  ; a continuación, pulse **Panel de instrumentos del rendimiento de aplicaciones**.
2. En el panel **Todas mis aplicaciones**, pulse una aplicación que desee supervisar; a continuación, pulse **Availability Monitoring** en el panel **Grupos**.

   Si no se listan aplicaciones, deberá crear una. Asegúrese de seleccionar **Aplicación personalizada** como **Plantilla**. Para obtener más información, consulte “Gestión de aplicaciones” en la página 1133.

   La pestaña **Visión general de estado** de Availability Monitoring visualiza tres indicadores que muestran el promedio de disponibilidad de prueba en las últimas 24 horas, el estado actual de todas las pruebas y el uso de servicio de su asignación para el plan actual.

   Puede configurar el modo en que Availability Monitoring calcula el promedio de disponibilidad de la prueba seleccionando pruebas para su inclusión en el **Cálculo de disponibilidad**. Pulse el icono de flecha en el indicador Promedio de disponibilidad de prueba para ver las tarjetas de prueba; a continuación, pulse **Cálculo de disponibilidad**. Pulse una tarjeta para añadirla o eliminarla del cálculo. Las tarjetas de prueba excluidas aparecen borrosas. Cuando haya terminado, pulse **Terminado**. El indicador Promedio de disponibilidad de prueba se renovará.

Puede ver el estado de todas las pruebas pulsando el icono de flecha en el indicador Estado de prueba actual. Se visualizarán tarjetas de prueba para las pruebas. Pulse una tarjeta para acceder al panel de instrumentos **Desglose** para esa prueba en particular.

3. Pulse **Ver detalles de supervisión** para acceder al panel de instrumentos de Availability Monitoring y ver datos para todas las pruebas de la aplicación. Pulse **Ver todas las pruebas** para ver y editar las pruebas en el panel **Pruebas sintéticas**. Pulse **Añadir nueva prueba** para crear una prueba.

   Nota: La primera vez que ejecuta Availability Monitoring, debe añadir una prueba para poder ver los datos del panel de instrumentos de Availability Monitoring.

Creación y configuración de pruebas

Crear y configurar pruebas que informan de la disponibilidad y el rendimiento de las aplicaciones web.

Cree y configure pruebas para supervisar el tiempo de disponibilidad y de respuesta de las aplicaciones con frecuencia desde varias ubicaciones geográficas. Ejecute pruebas sintéticas para medir el rendimiento de carga de sitios web y llamadas de API REST. Cree pruebas de comportamiento mediante script para ejecutar y supervisar scripts de Selenium que imitan flujos de usuarios en diferentes ubicaciones.

Creación de una prueba de API REST

Cree una prueba de API REST para probar el tiempo de respuesta y la disponibilidad de la aplicación web utilizando los siguientes métodos HTTP: GET, POST, PUT y DELETE.

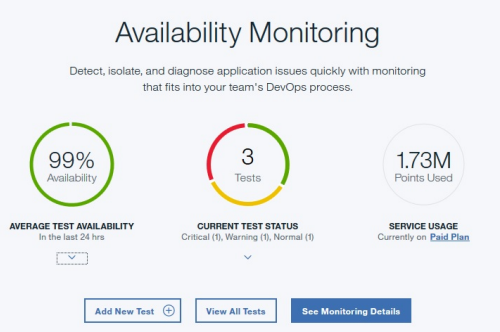
Acerca de esta tarea

Utilice las pruebas de API REST para supervisar la disponibilidad y el rendimiento de la aplicación web y otros URL en respuesta a llamadas REST.

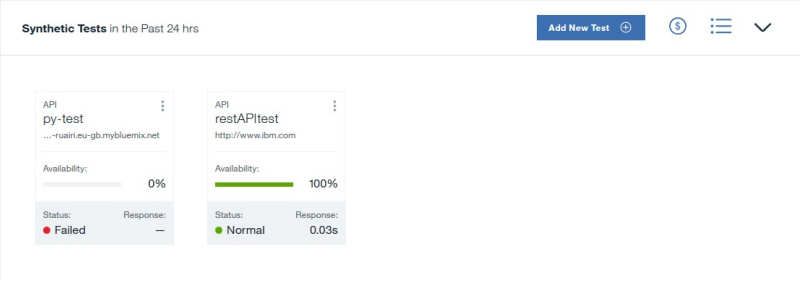
Procedimiento

Para crear una prueba de API REST, siga estos pasos.

1. Si está viendo la página de resumen de Availability Monitoring para la aplicación, pulse **Añadir nueva prueba**.



   Si está viendo el panel de instrumentos de Availability Monitoring, pulse **Añadir prueba nueva** en el panel **Pruebas sintéticas**.

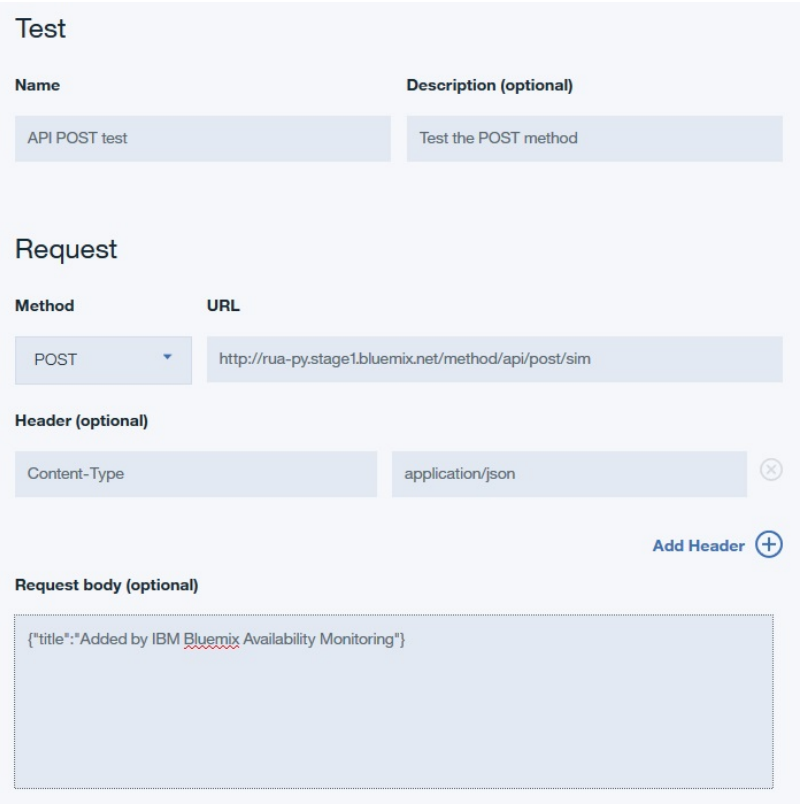


2. Pulse **Acción única** en la página **Configuración de supervisión**; a continuación, pulse **REST API** en la página **Acción única**.

3. Especifique un nombre significativo para la prueba en el campo **Nombre**. Añada una descripción de la finalidad de la prueba en el campo **Descripción**.
4. En la sección **Solicitud**, seleccione el tipo de método en la lista **Método** y especifique un **URL** que desee probar con este método.

   Puede elegir **GET**, **PUT**, **POST** o **DELETE**. Si elige el método **PUT** o **POST**, puede especificar el contenido del cuerpo para probar en el campo **Cuerpo de solicitud (opcional)**.

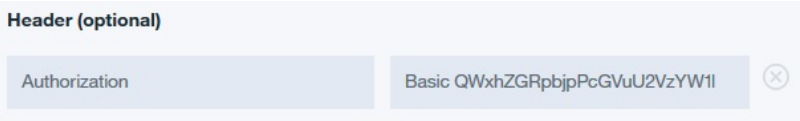
   Por ejemplo, la prueba de API REST siguiente utiliza el método POST para solicitar que la aplicación web acepte datos además de probar la disponibilidad y el rendimiento de dicha aplicación web.



5. Opcional: Configure la prueba para incluir una determinada cabecera y valor. Especifique un nombre y valor de cabecera en los campos **Cabecera**.

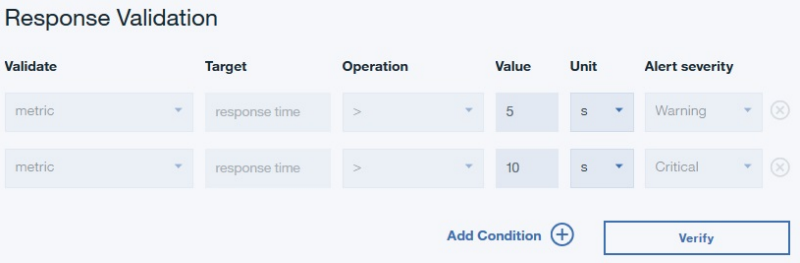
   Si la aplicación web que desea probar requiere un inicio de sesión y contraseña de usuario, especifique `"Autorización"` en el campo **Nombre de cabecera**. Especifique la palabra "Basic", un carácter de espacio y el valor codificado en base64 de *nombreusuario:contraseña* en el campo **Valor de cabecera**.

   Por ejemplo, si el nombre de usuario es *Aladdin* y la contraseña es *OpenSesame*, especifique la palabra "Basic", un carácter de espacio y el valor codificado en base64 para *Aladdin:OpenSesame* en el campo **Valor de cabecera**.



6. Configure los umbrales de alerta de aviso y crítica para la prueba en la sección **Validación de respuesta**. Edite el **Valor** y la **Unidad** para cada fila.

   Los tiempos de respuesta que superan los umbrales de aviso y críticos desencadenan alertas.



7. Opcional: Pulse **Añadir condición** para definir y añadir condiciones de validación de respuesta personalizadas.

   Las condiciones de validación de respuesta personalizadas se evalúan además de generar una alerta. Puede definir y añadir hasta seis condiciones personalizadas para la prueba.

   Importante:

   En Availability Monitoring cada prueba puede generar hasta un total de tres alertas. La prueba informa de la alerta con la gravedad más elevada hasta que se resuelven todas las condiciones que causan la alerta. Para obtener más información, consulte “Generación de alertas en Availability Monitoring” en la página 1094.

   Puede validar los datos siguientes:

   Código de respuesta de cabecera
   Seleccione **Código de respuesta de cabecera** para probar uno o un rango de códigos de respuesta HTTP.

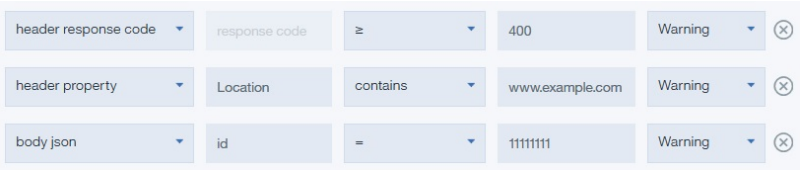
   Propiedad de cabecera
   Seleccione **Propiedad de cabecera** para probar una propiedad y valor de campo de cabecera HTTP determinado.

   Cuerpo JSON
   Seleccione **Cuerpo JSON** para probar una propiedad determinada de un cuerpo JSON.

   Para cada condición, especifique una propiedad para probarla en el campo **Destino** y un valor para probar en el campo **Valor**. Seleccione un operador del menú desplegable **Operación**. Finalmente, elija una **Gravedad de alerta** de Aviso o Crítica para la condición.

   Importante:

   Los valores numéricos que especifique en el campo **Valor** se tratarán como números y no como series de forma predeterminada. Para especificar un **Valor** para una condición de validación de respuesta, utilice comillas "" para distinguir entre una serie y un número. Por ejemplo, para probar la serie 123, especifique "123" en el campo **Valor**. Para comprobar el número 400, especifique 400 sin comillas.



8. Pulse **Verificar** para crear la prueba de API REST y determinar si su solicitud de prueba es válida.

   Availability Monitoring determina la validez de la prueba utilizando el método HTTP seleccionado y cualquier cabecera de solicitud que haya definido para la prueba. No se realiza ninguna validación de respuesta durante la verificación de la prueba.

   La prueba validada se visualiza en la tabla **Elementos verificados**. Puede añadir más URLs repitiendo los pasos 3 a 8.

9. Para configurar los valores de la prueba, pulse **Siguiente**.

   Se mostrará un resumen de la configuración de prueba. Se visualizará el mensaje siguiente para los valores predeterminados:

La prueba se realizará: cada 15 minutos en 3 ubicaciones públicas simultáneamente y ninguna ubicación privada para determinar si la prueba supera el umbral especificado.

10. En el panel **Configuración**, pulse **Editar** para visualizar los valores actuales para la prueba.

    Puede actualizar los siguientes valores:

    - **Intervalo** define la frecuencia de ejecución de la prueba.
    - **Frecuencia de prueba** determina si la prueba se ejecuta desde todas las ubicaciones simultáneamente o desde una ubicación diferente a cada intervalo. Seleccione **Simultánea** para ejecutar la prueba desde todas las ubicaciones simultáneamente, o **Escalonada** para ejecutar la prueba desde una ubicación seleccionada diferente en cada intervalo.
    - **Ubicaciones** determina las ubicaciones en las que se ejecuta la prueba.

11. Seleccione las ubicaciones en la lista de **Ubicaciones públicas**. Para seleccionar una ubicación privada desde la que ejecutar la prueba, primero debe instalar y configurar un PoP privado en la máquina desde la que desea ejecutar la prueba. Para obtener más información, consulte "Instalación y configuración de ubicaciones PoP privadas" en la página 1091.
12. Pulse **Guardar** para finalizar la configuración de la prueba; a continuación pulse **Finalizar**.

    Se muestra el panel de instrumentos Availability Monitoring. Después de un minuto, el panel de instrumentos mostrará información y datos para la nueva prueba.

Creación de una prueba de página web

Cree una prueba de página web para probar la disponibilidad de la aplicación web y supervisar cuánto tiempo tarda en abrirse esta página.

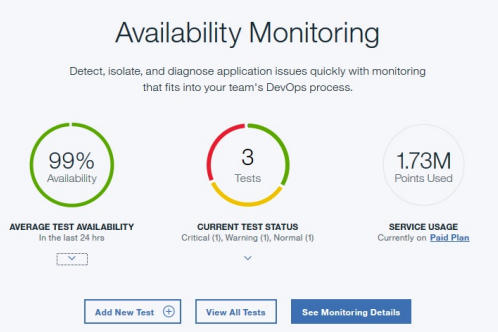
Acerca de esta tarea

Las pruebas de página web notifican el tiempo de respuesta necesario para cargar el URL de la aplicación web. Cree una prueba de página web para probar la disponibilidad y el tiempo de respuesta de la aplicación web.

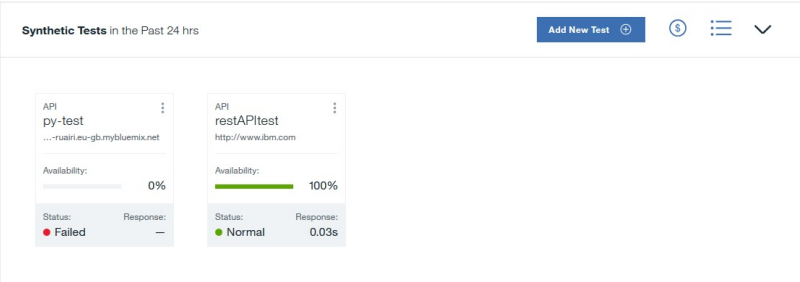
Procedimiento

Para crear una prueba de página web, siga estos pasos.

1. Si está viendo la página de resumen de Availability Monitoring, pulse **Añadir nueva prueba**.

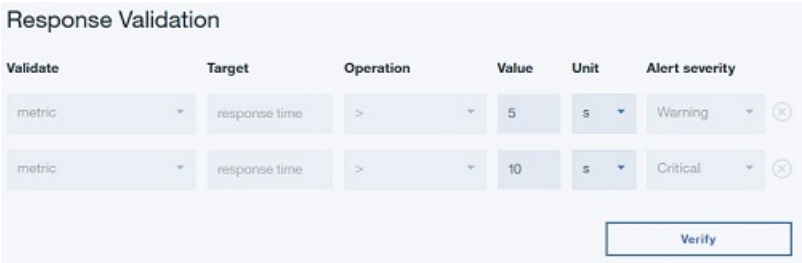


   Si está viendo el panel de instrumentos de Availability Monitoring, pulse **Añadir prueba nueva** en el panel **Pruebas sintéticas**.



2. Pulse **Acción única** en la página **Configuración de supervisión**; a continuación, pulse **Página web** en la página **Acción única**.
3. Especifique un nombre significativo para la prueba en el campo **Nombre**. Añada una descripción de la finalidad de la prueba en el campo **Descripción**.
4. Especifique el **URL** de la aplicación web que desea probar.
5. Configure los umbrales de alerta de aviso y crítica para la prueba en la sección **Validación de respuesta**. Edite el **Valor** y la **Unidad** para cada fila.

   Los tiempos de respuesta que superan los umbrales de aviso y críticos desencadenan alertas.



6. Utilice la **Lista negra** y la **Lista blanca** para especificar a qué URLs y dominios enviar solicitudes y qué URLs y dominios contribuyen a las métricas y el estado de las pruebas de aplicación. Añada los URLs y los dominios que desea incluir o bloquear a la **Lista blanca** y la **Lista negra**.

   Para obtener más información, consulte "Bloqueo y filtrado con la lista blanca y la lista negra" en la página 1089.
7. Pulse **Verificar** para crear la prueba de página web y determinar si su solicitud de prueba es válida.

   Availability Monitoring determina la validez de la prueba enviando una solicitud GET al URL de prueba. No se realiza ninguna validación de respuesta durante la verificación de la prueba.

   La prueba validada se visualiza en la tabla **Elementos verificados**. Puede añadir más URL repitiendo los pasos 3 a 7.
8. Para configurar los valores de la prueba, pulse **Siguiente**.

   Se mostrará un resumen de la configuración de prueba. Se visualizará el mensaje siguiente para los valores predeterminados:

   ```
   La prueba se realizará: cada 15 minutos en 3 ubicaciones públicas
   simultáneamente y ninguna ubicación privada para determinar si la prueba
   supera el umbral especificado.
   ```

   El uso estimado y el número estimado de pruebas por mes se muestra en función de la configuración de prueba actual.
9. En el panel **Configuración**, pulse **Editar** para visualizar los valores actuales para la prueba.

   Puede actualizar los siguientes valores:

   - **Intervalo** define la frecuencia de ejecución de la prueba.
   - **Frecuencia de prueba** determina si la prueba se ejecuta desde todas las ubicaciones simultáneamente o desde una ubicación diferente a cada intervalo. Seleccione **Simultánea** para ejecutar la prueba desde todas las ubicaciones simultáneamente, o **Escalonada** para ejecutar la prueba desde una ubicación seleccionada diferente en cada intervalo.
   - **Ubicaciones** determina las ubicaciones en las que se ejecuta la prueba.

   Seleccione las ubicaciones en la lista de **Ubicaciones públicas**. Para seleccionar una ubicación privada desde la que ejecutar la prueba, primero debe instalar y configurar un PoP privado en la máquina desde la que desea ejecutar la prueba. Para obtener más información, consulte "Instalación y configuración de ubicaciones PoP privadas" en la página 1091.

   Pulse **Guardar** para finalizar la configuración de la prueba.
10. Pulse **Finalizar**.

Se muestra el panel de instrumentos Availability Monitoring. Después de un minuto, el panel de instrumentos mostrará información y datos para la nueva prueba.

Creación de un script de prueba desde un script cargado

Cargue un script de Selenium para crear una prueba de script que pruebe la disponibilidad y el rendimiento de la aplicación web en respuesta al comportamiento simulado de los usuarios.

Antes de empezar

Para poder crear un script de prueba, primero debe crear un script de Selenium. Para obtener más información sobre la creación de scripts de Selenium, consulte Grabación de scripts sintéticos.

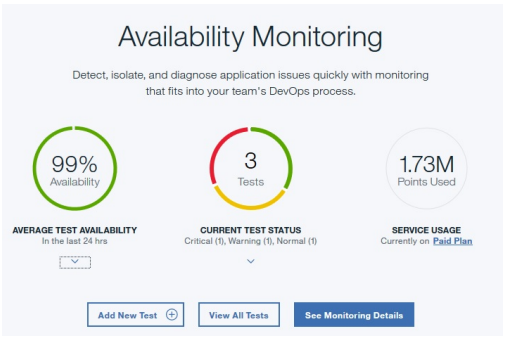
Acerca de esta tarea

Cree un script de prueba para supervisar un script de Selenium que simule las interacciones de los usuarios con la aplicación web. Si crea un script de Selenium que imita a un usuario que está iniciando la sesión en la aplicación, a continuación podrá ejecutar una prueba de script periódicamente para probar el rendimiento de la aplicación como respuesta a acciones de usuario simuladas.

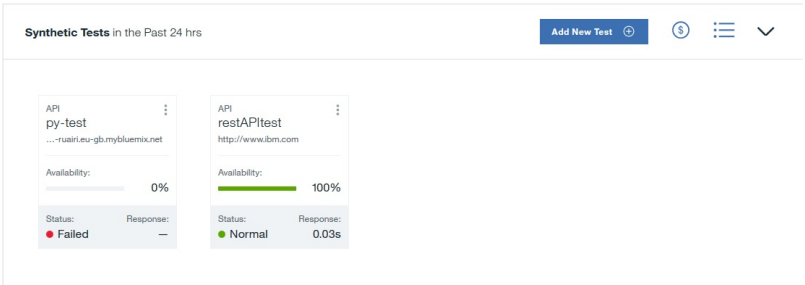
Procedimiento

Para crear un script de prueba, realice los pasos siguientes.

1. Si está viendo la página de resumen de Availability Monitoring, pulse **Añadir nueva prueba**.



   Si está viendo el panel de instrumentos de Availability Monitoring, pulse **Añadir prueba nueva** en el panel **Pruebas sintéticas**.



2. Pulse **Comportamiento programado** en la página **Configuración de supervisión**. Se visualizará la página **Configuración de comportamiento programado**. Pulse **Cargar archivo**.

   Si retrocede para editar esta prueba en un punto posterior, puede descargar el archivo de script cargado. Pulse el icono **Descargar** para descargar el script.
3. Especifique un nombre significativo para la prueba en el campo **Nombre**. Añada una descripción de la finalidad de la prueba en el campo **Descripción**.
4. Pulse **Examinar** para buscar y cargar un archivo de script.
5. Utilice la **Lista negra** y la **Lista blanca** para especificar a qué URLs y dominios enviar solicitudes y qué URLs y dominios contribuyen a las métricas y el estado de las pruebas de aplicación. Añada los URLs y los dominios que desea incluir o bloquear a la **Lista blanca** y la **Lista negra**.

Para obtener más información, consulte “Bloqueo y filtrado con la lista blanca y la lista negra” en la página 1089.

6. Para configurar los valores de la prueba, pulse **Siguiente**.

   Se mostrará un resumen de la configuración de prueba. Por ejemplo, se visualizará el mensaje siguiente para los valores predeterminados:

   ```
   La prueba se realizará: cada 15 minutos en 3 ubicaciones públicas
   simultáneamente y ninguna ubicación privada para determinar si la prueba
   supera el umbral especificado.
   ```

   El uso estimado y el número estimado de pruebas por mes se muestra en función de la configuración de prueba actual.

7. En el panel **Configuración**, pulse **Editar** para visualizar los valores actuales para la prueba.

   Puede actualizar los siguientes valores:

   - **Intervalo** define la frecuencia de ejecución de la prueba.
   - **Frecuencia de prueba** determina si la prueba se ejecuta desde todas las ubicaciones simultáneamente o desde una ubicación diferente a cada intervalo. Seleccione **Simultánea** para ejecutar la prueba desde todas las ubicaciones simultáneamente, o **Escalonada** para ejecutar la prueba desde una ubicación seleccionada diferente en cada intervalo.
   - **Umbral crítico** define el tiempo de respuesta para alertas críticas de la prueba.
   - **Umbral de aviso** define el tiempo de respuesta para alertas de aviso para la prueba.
   - **Ubicaciones** determina las ubicaciones en las que se ejecuta la prueba.

   Seleccione las ubicaciones en la lista de **Ubicaciones públicas** que se visualizan de forma predeterminada. Para seleccionar una ubicación privada desde la que ejecutar la prueba, primero debe instalar y configurar un PoP privado en la máquina desde la que desea ejecutar la prueba. Para obtener más información, consulte “Instalación y configuración de ubicaciones PoP privadas” en la página 1091.

   Si es necesario, puede especificar los valores para las variables definidas en el script de prueba. Por ejemplo, si el script necesita un nombre de usuario y una contraseña para realizar la conexión a un sitio web, puede indicar los valores para estas variables. Puede establecer valores diferentes para las variables en diferentes ubicaciones de la tabla **Variables de script**.

   Pulse **Guardar** para finalizar la configuración de la prueba.

8. Pulse **Finalizar**.

   Se muestra el panel de instrumentos Availability Monitoring. Después de un minuto, el panel de instrumentos mostrará información y datos para la nueva prueba.

Bloqueo y filtrado con la lista blanca y la lista negra

Utilice la lista blanca y la lista negra para determinar a qué recursos se envían solicitudes y qué recursos contribuyen a las métricas y al estado de las pruebas de la aplicación. Las listas blancas y las listas negras solo están disponibles para las pruebas de comportamiento de página de web y script.

Los campos **Lista blanca** y **Lista negra** definen los recursos a los que la prueba puede o no puede acceder y los recursos que contribuyen a las métricas y al estado de las pruebas. La Lista blanca y la Lista negra controlan qué dependencias y recursos contribuyen a los tiempos de respuesta de las aplicaciones web probadas, como por ejemplo métricas de terceros. Puede configurar la Lista blanca y la Lista negra cuando crea una prueba de comportamiento de página web o script.

Puede utilizar la **Lista blanca** para definir dominios y URL permitidos y a continuación utilizar la **Lista negra** para bloquear elementos específicos de las ubicaciones permitidas.

Sintaxis

Utilice comas (,) para separar elementos en la Lista negra y la Lista blanca. Utilice el símbolo de comodín (*) para filtrar elementos de cada URL o dominio.

Lista blanca

Añada URLs, esquemas o dominios que desea incluir en las solicitudes y los cálculos de métrica en el campo Lista blanca. Puede incluir hasta 10 elementos en la Lista blanca. La longitud de cada elemento no puede sobrepasar los 200 caracteres. Todos los dominios, esquemas y URLs que no coinciden con los elementos de la Lista blanca quedan bloqueados.

Por ejemplo: `ibm.com, *developerworks*, *.s81c.com/*, https://www.ibm.com*, https://*`

Nota: Si el filtro de URL de lista blanca incluye `http://` o `https://`, debe incluir el símbolo de comodín (*) directamente después del URL, por ejemplo, `https://www.ibm.com*`.

Lista negra

Añada URLs, esquemas o dominios que desea bloquear en las solicitudes y los cálculos de métricas en el campo Lista negra. Puede incluir hasta 20 elementos en la Lista negra. La longitud de cada elemento no puede sobrepasar los 200 caracteres.

Por ejemplo: `*.profile.*.cloudfront.net/*.png, http://*`

Nota: Si el filtro de URL de lista negra incluye `http://` o `https://`, debe incluir el símbolo de comodín (*) directamente después del URL, por ejemplo, `https://www.ibm.com*`.

Comportamiento de filtrado y bloqueo

Las pruebas pueden tener una Lista blanca y una Lista negra. A la hora de determinar qué ubicaciones están permitidas o bloqueadas, la Lista negra siempre prevalece sobre la Lista blanca. La tabla siguiente muestra el comportamiento de filtrado y de bloqueo de todos los escenarios que implican la Lista blanca y la Lista negra.

Tabla 253. Comportamiento de filtrado y de bloqueo para la Lista blanca y la Lista negra

Lista negra	Lista blanca	Comportamiento	Razón
Vacía	Vacía	Permitir acceso	No se han especificado reglas de filtrado.
Vacía	El URL no coincide con una entrada de la lista	Bloquear acceso	El URL no está en la lista blanca.
Vacía	El URL coincide con una entrada de la lista	Permitir acceso	El URL está en la lista blanca. No hay ninguna entrada de la lista negra que bloquee el acceso.
El URL no coincide con una entrada de la lista	Vacía	Permitir acceso	El URL no está en la lista negra. No hay entrada en la lista blanca para impedir el acceso a URLs que no estén en la lista blanca.
El URL coincide con una entrada de la lista	Vacía	Bloquear acceso	El URL está en la lista negra.
El URL no coincide con una entrada de la lista	El URL no coincide con una entrada de la lista	Bloquear acceso	El URL no está en la lista blanca.
El URL no coincide con una entrada de la lista	El URL coincide con una entrada de la lista	Permitir acceso	El URL está en la lista blanca. El URL no está en la lista negra.

Tabla 253. Comportamiento de filtrado y de bloqueo para la Lista blanca y la Lista negra (continuación)			
Lista negra	**Lista blanca**	**Comportamiento**	**Razón**
El URL coincide con una entrada de la lista	El URL no coincide con una entrada de la lista	Bloquear acceso	El URL no está en la lista blanca. El URL está en la lista negra.
El URL coincide con una entrada de la lista	El URL coincide con una entrada de la lista	Bloquear acceso	El URL está en la lista negra. La entrada de la lista negra prevalece sobre la entrada de la lista blanca.

Instalación y configuración de ubicaciones PoP privadas

Descargue e instale un PoP privado en una máquina local; a continuación, configure el PoP privado para utilizarlo como ubicación para las pruebas en Availability Monitoring.

Antes de empezar

Para instalar un PoP privado, la ubicación de instalación del PoP privado debe cumplir los requisitos siguientes:

- Linux debe estar instalado con una versión de kernel 3.1.0 o posterior.
- El servicio de Docker versión 1.7.1 o superior debe estar instalado e iniciado.
- El espacio de disco disponible debe ser de 4 GB o más.
- La memoria disponible debe ser de 2 GB o más.
- Núcleos de CPU:
  - Si sólo necesita reproducciones de API REST en el PoP privado, debe disponer de 2 núcleos de CPU disponibles como mínimo.
  - Si desea ejecutar reproducciones de páginas web y reproducciones de script en el PoP privado, debe disponer de 1 núcleo de CPU para cada 1 o 2 pruebas para que se ejecuten cada minuto.
- Compruebe el uso de CPU y memoria del PoP privado antes y después de añadir nuevas pruebas, y después de aplicar actualizaciones de software de PoP privado que incluyan versiones actualizadas de Firefox o el IDE de Selenium, ya que las versiones posteriores podrían tener requisitos de sistema más elevados.

La mejor práctica para determinar cuándo añadir núcleos de CPU es ejecutar el proceso más exigente en el host de PoP privado para obtener el uso de CPU y de memoria: si el uso de CPU total es superior al 70% y el proceso de mayor uso de CPU es Firefox, añada núcleos de CPU hasta que el uso de CPU total esté por debajo del 50%; si la memoria libre del host de PoP privado está por debajo de 500 MB, aumente la memoria.

Si no tiene más recursos de hardware, pero desea que el PoP privado se ejecute sin excepción, siga estos pasos para reducir el número de instancias de ejecución paralela de Firefox (que hace que las pruebas se ejecuten con intervalos más largos que los configurados en la interfaz de usuario porque el recurso de hardware no puede ejecutar muchas pruebas):

1. Edite el script `start-pop.sh` para añadir la variable de entorno **`MAX_TASKPOOL_SIZE`**, especificando los núcleos de CPU disponibles en el host de PoP privado como valor y, a continuación, ejecute **`stop-pop.sh`** seguido de **`start-pop.sh`**.
2. Establezca las pruebas en un intervalo más largo en la IU.

Debe tener acceso de usuario a la interfaz de línea de mandatos (CLI) de la máquina en la que desea instalar el PoP privado. También debe tener los permisos de usuario necesarios para añadir paquetes a Docker.

Importante:

- Asegúrese de que la hora del sistema de la máquina donde desea ejecutar un PoP privado está y permanece sincronizada con la hora estándar. De lo contrario, las instancias de prueba muestran indicaciones de fecha y hora incorrectas en el panel de instrumentos de Availability Monitoring.
- El PoP privado de Availability Monitoring está totalmente soportado para las plataformas siguientes: Red Hat Enterprise Linux 7.4 y CentOS Linux 7.4.

Acerca de esta tarea

Además de las ubicaciones públicas, puede desplegar puntos de presencia (PoP) privados al crear o editar una prueba en Availability Monitoring. Utilice PoP privados para probar aplicaciones que se encuentran detrás del cortafuegos de la empresa, como por ejemplo aplicaciones con mayores requisitos de privacidad o seguridad. Puede registrar un máximo de 50 ubicaciones privadas en Availability Monitoring. Descargue el script de comprobación previa y el paquete de PoP privado; a continuación, guarde el script y el paquete en la máquina en la que desea ejecutar el PoP privado.

Procedimiento

1. Cree una prueba o edite una prueba existente.

   Para crear una prueba, pulse **Añadir nueva prueba** en el panel **Pruebas sintéticas**. Para editar una prueba, pulse **Acciones** ⋮ ; a continuación, pulse **Editar**. Si está creando una prueba, configure y verifique la prueba. En la sección **Valores**, pulse **Editar**.

   Para obtener más información, consulte los apartados "Creación de una prueba de API REST" en la página 1083, "Creación de una prueba de página web" en la página 1086 y "Creación de un script de prueba desde un script cargado " en la página 1088.
2. Pulse **Editar** en la sección **Configuración** para visualizar la sección **Ubicaciones**; a continuación, pulse **Ubicaciones privadas**. Si está editando una prueba anterior, pulse **Ubicaciones privadas** en la sección **Ubicaciones**.

   Si anteriormente ha instalado uno o varios PoP privados, se visualiza una lista de todos los PoP privados instalados. Si no se han instalado y configurado PoP privados, Availability Monitoring puede guiarle en la configuración de un PoP privado.
3. Pulse **Descargar comprobación previa** y guarde el script de comprobación previa en una máquina desde la que desea ejecutar pruebas.

   Importante: Debe extraer y ejecutar los scripts desde la interfaz de línea de mandatos (CLI) para instalar un PoP privado. Los scripts y el paquete de PoP privado se pueden instalar en una máquina distinta y se puede acceder a ellos a través de la CLI para esa máquina. No cierre ni renueve Availability Monitoring en el navegador mientras esté trabajando con scripts de PoP privados, ya que perderá los valores de prueba no guardados.

   Abra una CLI para la máquina en la que desea ubicar el PoP privado. Desde la CLI, vaya a la ubicación donde ha guardado el script de precomprobación; a continuación, ejecute el script de precomprobación del siguiente modo:

   ```
   ./precheck.sh
   ```

   Asegúrese de que tiene los permisos necesarios para ejecutar scripts de shell en la máquina.

   El script de precomprobación muestra el resultado de la comprobación. Si el entorno falla la comprobación, actualice la máquina para que cumpla los requisitos que se visualizan.
4. Vuelva a Availability Monitoring, pulse **Descargar paquete** y guarde el paquete. Mueva el paquete a la máquina desde la que desea ejecutar pruebas. En la CLI, vaya a la ubicación en la que ha guardado el paquete descargado; a continuación, ejecute el mandato para extraer el paquete:

   ```
   tar -xvf Availability_Monitoring_PoP.tar
   ```

   Donde *Availability_Monitoring_PoP.tar* es el nombre del archivo `.tar` que contiene el paquete PoP privado que ha descargado.
5. Configure el PoP privado. En la CLI, ejecute el script siguiente:

```
./config-pop.sh
```

Cuando se le solicite, especifique la siguiente información para el PoP privado:

- Nombre de PoP
- Ubicación de país
- Ubicación de ciudad
- Latitud de PoP
- Longitud de PoP
- Descripción de PoP

6. Si alguna de las pruebas de API REST se conecta a un servidor que utiliza un certificado autofirmado o que no está firmado por un proveedor de certificados de autoridad emisora de certificados (CA) conocido, coloque los certificados de CA de confianza que estén en el formato de archivo `.pem` en el directorio `keyfiles`.

   Nota:

   - Los cambios en los archivos de certificado `.pem` requerirán el reinicio del PoP privado.
   - El servidor que se está probando debe enviar todos los certificados, excepto el certificado de CA raíz, durante el reconocimiento de TLS; si esto no ocurre, corrija la configuración del servidor si es posible. En caso contrario, puede añadir los certificados que falten al directorio `keyfiles` tal como se describe en este paso. Sin embargo, es posible que la prueba (o pruebas) de PoP no refleje la experiencia de otros clientes.

7. Para configurar el PoP privado para que utilice un servidor proxy cuando se ejecutan pruebas de página web o pruebas de comportamiento por script, especifique una de las opciones siguientes:

   Importante: las pruebas de API REST que se ejecutan desde su ubicación PoP privada con una configuración de proxy manual o automática no utilizan ese proxy. Sólo las pruebas de página web y de comportamiento por script pueden utilizar un servidor proxy para ejecutarse desde ubicaciones PoP privadas.

   no
   Especifique no para configurar el PoP privado de modo que no utilice un proxy cuando se ejecutan las pruebas.

   manual
   Especifique `manual` para configurar manualmente una dirección IP y número de puerto de proxy para el proxy PoP privado que debe utilizarse cuando se ejecutan las pruebas. El script solicita la dirección IP y el número de puerto del servidor proxy en el formato siguiente: *`dirección ip:número de puerto`*. También puede crear una lista sin proxy para bloquear elementos de dominio, nombres de host o elementos de dirección IPv4. Cuando se le solicite, especifique uno o varios elementos de dominio o elementos de dirección IPv4. Separe cada elemento de la lista con un espacio en blanco o una coma (","). El operador comodín (*) no está soportado.

   - Para bloquear un dominio y los subdominios, especifique un sufijo de dominio que empiece por un punto, por ejemplo: `.example.org, example.org`.
   - Para bloquear una red, especifique una dirección IP con un sufijo CIDR para identificar un rango de direcciones IP a bloquear, por ejemplo: `10.0.0.0/8`.

   pac
   Especifique `pac` para configurar el PoP privado para que utilice un URL de configuración de proxy automático. Cuando se lo solicite el script, especifique el URL de configuración de proxy automático.

   Los valores de PoP privado se guardan en el archivo `pop.properties`.

8. Inicie el PoP privado. En la CLI, ejecute el script siguiente:

   ```
   ./start-pop.sh
   ```

   Cuando el PoP privado esté en ejecución, Availability Monitoring podrá encontrarlo.

9. Vuelva a Availability Monitoring y pulse  **Renovar ubicaciones** para buscar y visualizar el PoP privado nuevo.

   El PoP privado aparece en una tabla.
10. Para elegir el PoP privado como ubicación para la prueba, marque el recuadro de selección de la fila de la tabla que contiene un PoP privado. Para suprimir un PoP privado, siga estos pasos:
    a) En la CLI, ejecute el script **`./stop-pop.sh`** en la máquina en la que se encuentra el PoP privado.
    b) Vuelva a Availability Monitoring y pulse  **Suprimir** en la fila de la tabla que contiene el PoP privado que desea suprimir.
11. Repita los pasos 3 a 10 para añadir más PoP privados a máquinas diferentes para su selección como ubicaciones en Availability Monitoring. Pulse **Finalizar** para guardar e iniciar la prueba.

    Se muestra el panel de instrumentos Availability Monitoring. Después de aproximadamente un minuto, el panel de instrumentos mostrará información y datos para la nueva prueba.
12. Opcional: Para actualizar un PoP privado existente, siga estos pasos:
    a) Descargue el nuevo paquete del PoP privado en una carpeta nueva; a continuación, utilice el mandato **`tar -xvf`** para desempaquetar el nuevo PoP en esa carpeta.
    b) En la CLI, cambie de directorio a la carpeta donde se encuentra el antiguo PoP privado. Ejecute el script siguiente para detener el PoP privado antiguo:

       `./stop-pop.sh`
    c) En el directorio en el que está ubicado el PoP privado antiguo, haga una copia de seguridad de los archivos `system.properties` y `pop.properties` existentes.

       Importante: El archivo `system.properties` contiene información crítica que permite al PoP privado conectarse con el Servidor de Cloud APM. El archivo `pop.properties` contiene los datos de configuración del PoP privado. Si desea retener eta configuración, asegúrese de conservar los archivos `pop.properties` y `system.properties` correspondientes al PoP privado antiguo antes de actualizar el PoP privado.
    d) Copie todos los archivos de la nueva carpeta del PoP privado excepto `pop.properties` y `system.properties` y sustituya los archivos de la ubicación del PoP privado antiguo.
    e) Si necesita reconfigurar el PoP privado actualizado, ejecute el script siguiente desde la CLI:

       `./config-pop.sh`
    f) Ejecute **`./start-pop.sh`** desde la CLI para iniciar el PoP privado actualizado.
    g) Vuelva a Availability Monitoring y pulse  **Renovar ubicaciones** para buscar y visualizar el PoP privado actualizado.

Generación de alertas en Availability Monitoring

En Availability Monitoring, las pruebas pueden generar un máximo de tres alertas en total. La prueba informa de la alerta con la gravedad más elevada hasta que se resuelve la condición que causa la alerta.

Se genera una alerta por separado para tres situaciones diferentes:

- Cuando el tiempo de respuesta de la aplicación web o URL supera los umbrales de aviso o crítico establecidos para la prueba. Cada prueba mide el tiempo de respuesta predeterminado y genera una alerta en función de los umbrales de aviso y crítico para esa prueba.
- Cuando la prueba devuelve un código de respuesta HTTP que indica que la aplicación web o el URL no está disponible debido a un error de cliente o servidor. Cada prueba busca el código de respuesta predeterminado para determinar si la prueba es satisfactoria o falla.
- Cuando prueba determina que se satisface una o más condiciones personalizadas, se genera una alarma con la mayor gravedad definida por una o varias de las condiciones personalizadas. Availability Monitoring tiene en cuenta la suma de todas las condiciones personalizadas al determinar si se genera

una alarma. Esta alarma permanece hasta que la prueba determina que todas las condiciones personalizadas ya no generan ninguna alerta de aviso o crítica.

Cuando salta más de una alerta, Availability Monitoring informará de la alerta cuya gravedad sea más alta mientras haya alertas presentes.

Por ejemplo, si añade una condición personalizada que genera una alerta crítica y otra condición personalizada que genera una alerta de aviso, la prueba genera una alerta crítica. Esta alerta es visible en el panel de instrumentos de Availability Monitoring. Si la condición que provoca una alerta crítica ya no se cumple, la gravedad de la alerta de prueba cambia a "aviso". Una alerta permanece hasta que ninguna de las condiciones causa una alerta.

Visualización de la disponibilidad y el rendimiento de la aplicación en el panel de instrumentos de supervisión

Puede ver los detalles de disponibilidad y rendimiento de la aplicación, junto con las alertas y las pruebas asociadas, en el panel de instrumentos de Availability Monitoring.

El panel de instrumentos de Availability Monitoring se divide en los paneles siguientes:

- Resumen de aplicación
- Frecuencia de alertas
- Pruebas sintéticas
- Tiempo de respuesta y disponibilidad

Utilice el menú desplegable **Navegar a** 

para navegar rápidamente a cualquier panel.

Utilice las guías como ayudar para conocer las características de Availability Monitoring. Para abrir una guía, pulse el icono **Ayuda** ; a continuación, pulse la guía que desea ver.

Biblioteca de guías de aprendizaje en vídeo
La biblioteca de guías de aprendizaje en vídeo contiene vídeos de aprendizaje sobre cómo crear pruebas de Availability Monitoring, crear scripts de prueba con Selenium IDE y enviar alertas.

Bienvenido a Monitoring
La guía Bienvenido a Monitoring destaca las áreas del panel de instrumentos y describe cada característica de Availability Monitoring.

Puede acceder al panel de instrumentos **Desglose** desde el panel Resumen de aplicación, el panel Frecuencia de alertas, el panel Pruebas sintéticas o el panel Tiempo de respuesta y disponibilidad. El panel de instrumentos **Desglose** muestra información estadística clave para las instancias de prueba.

Puede modificar el orden de los paneles para ajustarlo a sus necesidades. Para mover un panel, pulse la cabecera y arrastre el panel a una posición distinta. Para guardar estos cambios y que se conserven después de cerrar sesión, pulse **Guardar diseño**.

Puede establecer el panel de instrumentos para que se renueve automáticamente cada minuto. Pulse el icono **Configurar** ; a continuación, pulse la barra de deslizamiento de **Renovar** para seleccionar **1 minuto**. Para renovar la página en cualquier momento, pulse **Renovar**.

Resumen de aplicación
El panel Resumen de aplicación muestra una visión general del estado de alertas durante las últimas 24 horas y la información de estado de prueba actual.

El panel Resumen de aplicación muestra la información siguiente:

- **Estado actual** visualiza el estado de gravedad más elevado de todas las pruebas. La gravedad puede ser Normal, Aviso o Crítica.
- **Alertas** muestra el número de alertas abiertas y las divide en alertas de aviso y alertas críticas.

- **Informe de disponibilidad** permite descargar un informe en archivo `.csv` de los promedios de tiempo de respuesta y disponibilidad mensual, semanal y diaria de la aplicación. Pulse el icono **Informe** para descargar el informe.

Frecuencia de alertas
El panel **Frecuencia de alertas** contiene un mapa que muestra las alertas más recientes. Las alertas se agrupan por ubicación y se listan en la tabla **Alertas**.

Mapa de frecuencia de alertas

El mapa de **Frecuencia de alertas** muestra información general para todos los puntos de presencia (PoP) públicos y privados para las pruebas.

Utilice la función de zoom para ampliar cualquier área del mapa o restaurarlo en su tamaño original. Pase el cursor por encima de cada ubicación para ver el nombre de esa ubicación y el número de alertas de aviso y críticas en esa ubicación. Puede filtrar las alertas que se muestran en el mapa seleccionando **Todas**, **Abiertas** o **Cerradas** en la lista desplegable **Alertas**.

Ubicaciones PoP

Los iconos de **Ubicación PoP** 

indican las ubicaciones de PoP de las pruebas. El color de cada icono de **ubicación PoP** representa la gravedad de la alerta más reciente en cada ubicación: Normal, 

, Aviso, 

o Crítica 

. Un icono de **ubicación PoP** animado icono indica que esta ubicación contiene la mayoría de alertas con el nivel de gravedad más alto de todas las ubicaciones de las instancias de prueba.

Añada ubicaciones PoP a la prueba seleccionada pasando el cursor por encima de un icono de **Ubicación PoP inactiva**  y pulsando **Probar aquí**. Se visualizará la página **Modalidad de edición de prueba** para la prueba seleccionada. Puede seleccionar una prueba desde el menú desplegable **Probar** del panel **Tiempo de respuesta** y **Disponibilidad**.

Las ubicaciones PoP privadas están representadas por iconos de **Ubicación PoP privada** 

Número de alertas
Los iconos de **Ubicación PoP** visualizan el número de alertas abiertas, cerradas o todas las alertas generadas en cada ubicación. Los iconos **Crítico**, **Aviso** y **Normal**


visualizan el número de alertas de cada gravedad de las ubicaciones.

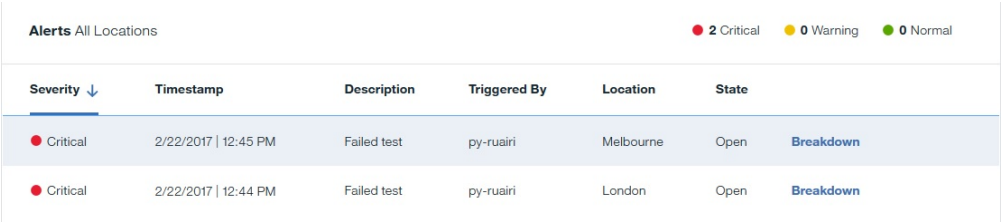
Pruebas erróneas
Las ubicaciones donde se producen pruebas erróneas están indicadas por un icono de **Ubicación PoP** con una marco 

.

Utilice la función de zoom para ampliar cualquier área del mapa o restaurarlo en su tamaño original. Pase el cursor por encima de cada ubicación para ver el nombre de esa ubicación y el número de alertas de aviso y críticas en esa ubicación. Puede filtrar las alertas que se muestran en el mapa seleccionando **Todas**, **Abiertas** o **Cerradas** en la lista desplegable **Alertas**.

Tabla de alertas

Las alertas de todas las ubicaciones se visualizan en una tabla.



La tabla muestra la siguiente información sobre las alertas:

- **Gravedad** describe la alerta como crítica o de aviso.
- **Indicación de fecha y hora** muestra la hora de creación de la alerta.
- **Descripción** resume el rendimiento de la instancia de prueba.
- **Desencadenada por** muestra el nombre de la prueba que ha desencadenado la alerta.
- **Ubicación** indica dónde se ha producido el problema.
- **Estado** muestra si la alerta está abierta o cerrada.

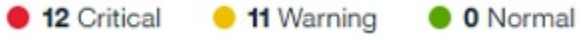
Visualización de detalles de alerta

Cada alerta de la tabla contiene un enlace al panel de instrumentos **Desglose**. Utilice el panel de instrumentos de desglose como ayuda para resolver el problema que causó la alerta.

Filtrado de alertas

Para filtrar las alertas de una ubicación concreta, pulse un icono **Ubicación PoP** en el mapa. Para mostrar las alertas de todas las ubicaciones, pulse en cualquier punto del mapa que no sea un icono **Ubicación PoP**.

Para filtrar las alertas de la tabla por gravedad, pulse el icono **Crítico**, **Aviso** o **Normal**



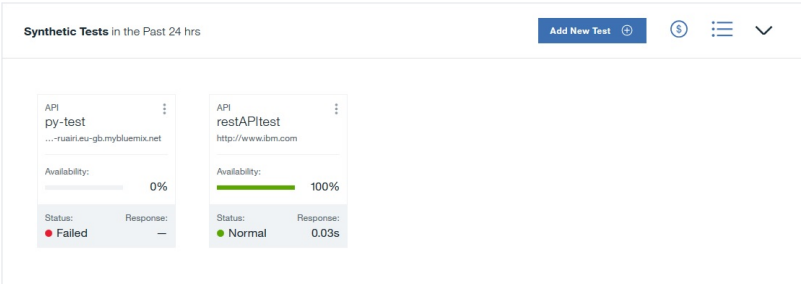
. Para eliminar el filtro e incluir las alertas de cada gravedad en la tabla, pulse de nuevo el icono seleccionado.

Cambio de umbrales de alerta

Las alertas son desencadenadas por los umbrales que ha especificado al crear una prueba. En la mayoría de los casos, se generan debido a errores de disponibilidad o tiempos de respuesta lentos. Para cambiar los valores del umbral, pulse el icono **Acciones** en la prueba que ha generado la alerta en el panel **Pruebas sintéticas** y pulse **Editar**.

Pruebas sintéticas

En el panel **Pruebas sintéticas**, puede crear, editar, suprimir y ver *pruebas sintéticas* que supervisan el rendimiento y la disponibilidad de las aplicaciones. Las pruebas se muestran en una lista o vista de tarjeta en el panel **Pruebas sintéticas**.



Cada tarjeta de prueba visualiza información sobre la prueba:

Disponibilidad
Visualiza el porcentaje de disponibilidad de la prueba durante las últimas 24 horas.

Estatus
Visualiza el estado actual de la prueba. El estado puede ser Crítico, Aviso, Normal, Fallido, Inactivo o Desconocido.

Promedio de respuesta
Visualiza el tiempo de respuesta promedio de la prueba durante las últimas 24 horas.

Puede supervisar tres tipos distintos de pruebas:

API REST
Indica el tiempo de respuesta de una llamada REST. Se admiten todos los formatos de solicitud HTTP, como GET, POST, PUT y DELETE.

Página web
Indica el tiempo de respuesta de la carga del sitio web en el URL especificado.

Comportamiento programado
Supervisa scripts de Selenium creados para imitar las interacciones de un usuario en un sitio web. Por ejemplo, puede crear un script de Selenium que imite a un usuario que está iniciando sesión en la aplicación. Ejecute este script periódicamente para probar el rendimiento de la app como respuesta a acciones del usuario que se automatizan con el script. Para obtener más información sobre la creación de scripts de Selenium, consulte “Grabación de scripts sintéticos” en la página 1062.

Para añadir otra prueba, pulse **Añadir nueva prueba**.

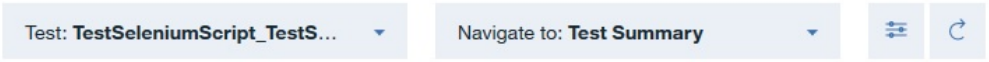
Para detener, iniciar, suprimir o editar una prueba sintética, pulse el icono **Acciones** y pulse la acción que desee llevar a cabo. Para ver los detalles de **Desglose** de la prueba, pulse la prueba.

Para ver el uso específico de cada prueba sintética, pulse el icono **Coste** . Si está suscrito al plan prepagado, su uso se visualiza en puntos de datos.

Desglose
El panel de instrumentos **Desglose** muestra información estadística clave para las pruebas. El panel de instrumentos también resume la información de disponibilidad y de tiempo de respuesta, las tendencias históricas y los datos de rendimiento de prueba en las 24 horas anteriores.

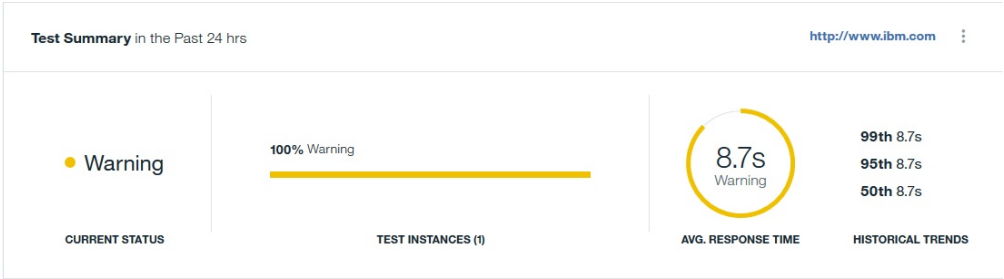
Para ver un desglose detallado de una prueba, pulse la prueba en el panel **Pruebas sintéticas**. También puede abrir el panel de instrumentos **Desglose** pulsando **Desglose** en la tabla **Alerta** del panel Frecuencia de alerta.

Utilice el menú desplegable **Prueba** para ver desgloses de pruebas diferentes. Utilice el menú desplegable **Navegar a** para navegar rápidamente a cualquier panel.



El panel de instrumentos Desglose muestra cuatro paneles.

Resumen de prueba

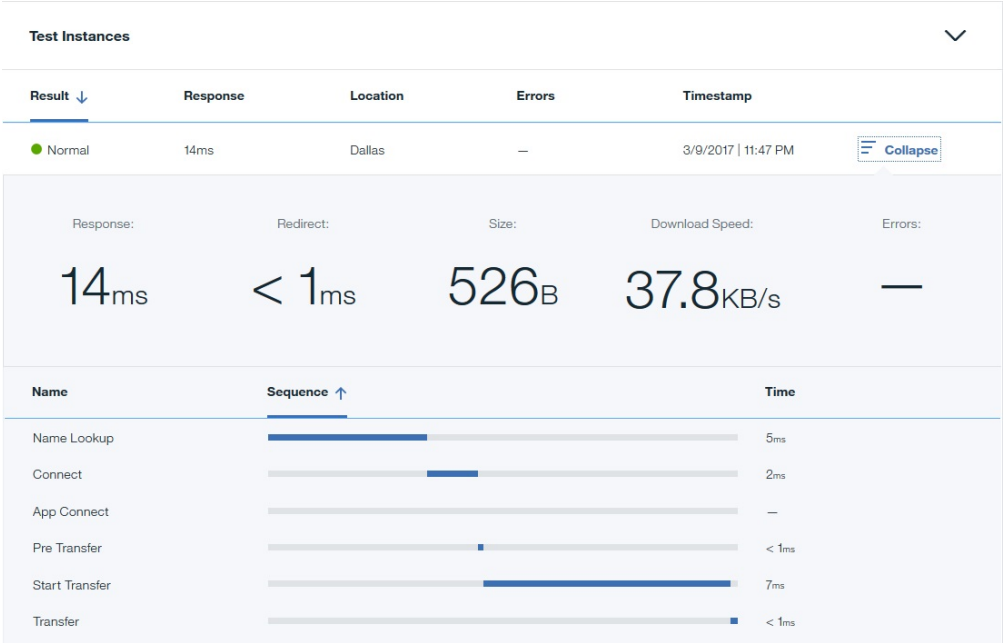


El panel **Resumen de prueba** muestra la información de prueba siguiente para las últimas 24 horas:

- **Estado actual** muestra el estado de la prueba.

- **Instancias de prueba** muestra un desglose del porcentaje de las instancias de prueba críticas, de aviso y normales.
- **Tiempo de respuesta promedio** muestra el tiempo de respuesta medio de la prueba.
- **Tendencias históricas** muestra las tendencias históricas del rendimiento de prueba para los percentiles 50º, 95º y 99º en segundos o milisegundos.

Instancias de prueba



En la tabla **Instancias de prueba** se muestra información detallada sobre cada instancia de prueba, incluidos el estado, el tiempo de respuesta, la ubicación donde se ha ejecutado la prueba, el número de errores y la indicación de fecha y hora en la que se ha ejecutado la prueba. Para obtener más detalles de una instancia de prueba, pulse **Expandir**. Se lista la información de respuesta detallada para cada paso de la instancia de prueba. Puede ordenar las columnas e identificar con rapidez el paso concreto en el que se ha producido el error o la ralentización. Visualizar los errores, la secuencia de prueba y el tiempo de respuesta ayuda a identificar problemas.

La información que se muestre dependerá del tipo de prueba sintética que se esté supervisando:

API

Al pulsar **Expandir** para una instancia de prueba de API, se visualiza un resumen genérico de los siguientes detalles:

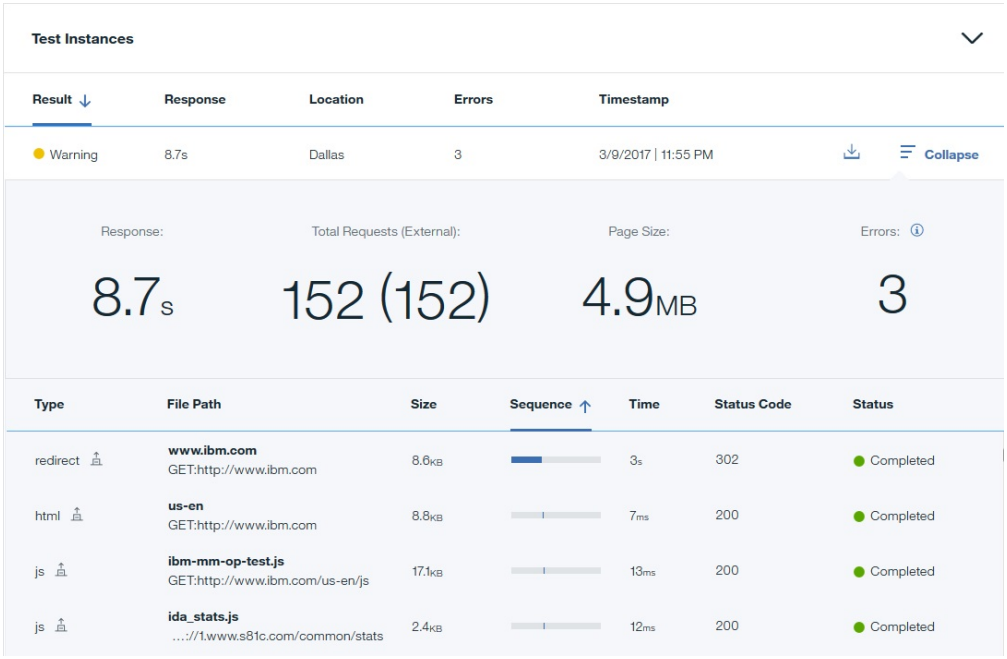
- **Respuesta** muestra el tiempo de respuesta total para la instancia de prueba, incluido el tiempo de redirección.
- **Redirección** muestra el tiempo total de redirección de la instancia de prueba.
- **Tamaño** muestra el tamaño del objeto.
- **Velocidad de descarga** muestra la velocidad a la que se descarga cada objeto.
- **Errores** muestra el número de errores que se han producido durante la instancia de prueba. Para ver los detalles de error, pulse el icono **Información**.

Una tabla muestra cada paso de la llamada de API, junto con el nombre del paso, la secuencia de pasos y el tiempo de respuesta de cada paso. Se visualizan los siguientes nombres de paso:

- **Búsqueda de nombre** representa el tiempo que la instancia de prueba ha tardado en resolver el nombre del objeto.
- **Conexión** representa el tiempo que la instancia de prueba ha tardado desde el principio del paso hasta que se ha completado una conexión al proxy o host remoto.

- **Conexión de aplicación** representa el tiempo que la instancia de prueba ha tardado desde el principio del paso hasta que se ha completado la conexión SSL al host remoto.
- **Pretransferencia** representa el tiempo que la instancia de prueba ha tardado desde el principio del paso hasta inmediatamente antes de que se inicie el mandato de transferencia de archivos.
- **Iniciar transferencia** representa el tiempo que la instancia de prueba ha tardado desde el principio del paso hasta que se ha recibido el primer byte.
- **Transferencia** representa el tiempo que la instancia de prueba ha tardado en transferir el archivo.

Página web



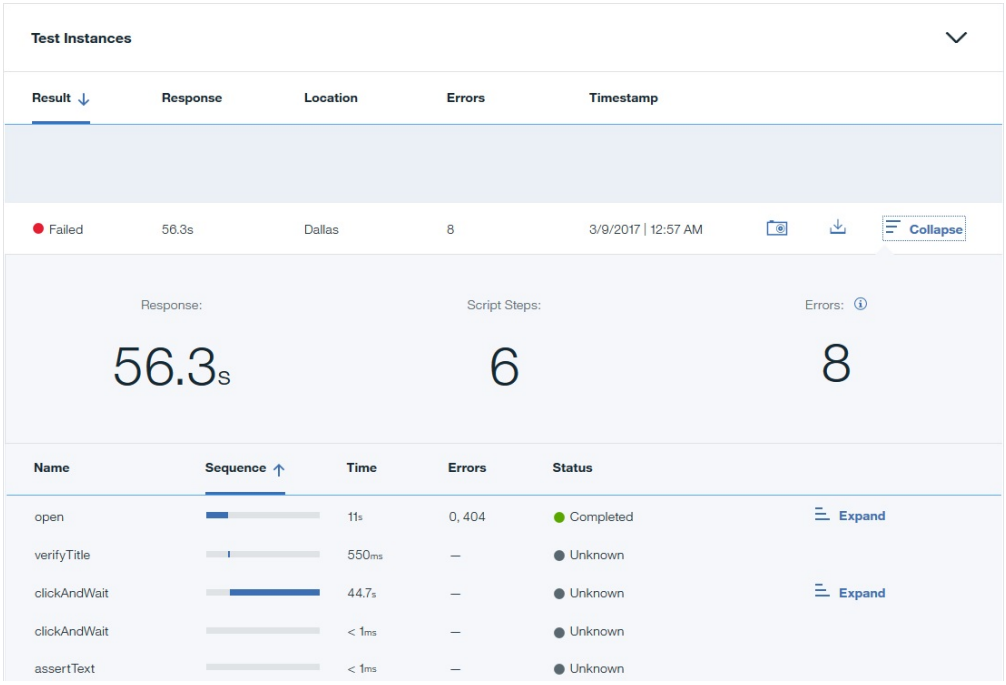
Al pulsar **Expandir** para una instancia de prueba de página web, se visualiza un resumen genérico de los siguientes detalles:

- **Respuesta** indica el tiempo de respuesta de la instancia de prueba.
- **Total de solicitudes (Externas)** muestra el número total de solicitudes de la instancia de prueba. El número de solicitudes externas está entre paréntesis.
- **Tamaño de página** muestra el tamaño de la página web.
- **Errores** muestra el número de errores que se han producido durante la instancia de prueba. Para ver los detalles de error, pulse el icono **Información**.

También se visualiza una tabla que muestra los siguientes detalles para cada solicitud realizada por la prueba:

- **Tipo** muestra el tipo de solicitud, por ejemplo, HTML, CSS, JavaScript o imagen. Las solicitudes externas e internas están representadas por iconos.
- **Vía de acceso de archivo** describe la ubicación del objeto solicitado.
- **Tamaño** muestra el tamaño del objeto solicitado.
- **Secuencia** muestra la secuencia de solicitudes realizadas por la prueba.
- **Tiempo** muestra el tiempo que tarda cada solicitud.
- **Código de estado** muestra el código de estado de solicitud HTTP.
- **Estado** describe el resultado de la solicitud, por ejemplo, Completada, Desconocido o Anómala.

Script

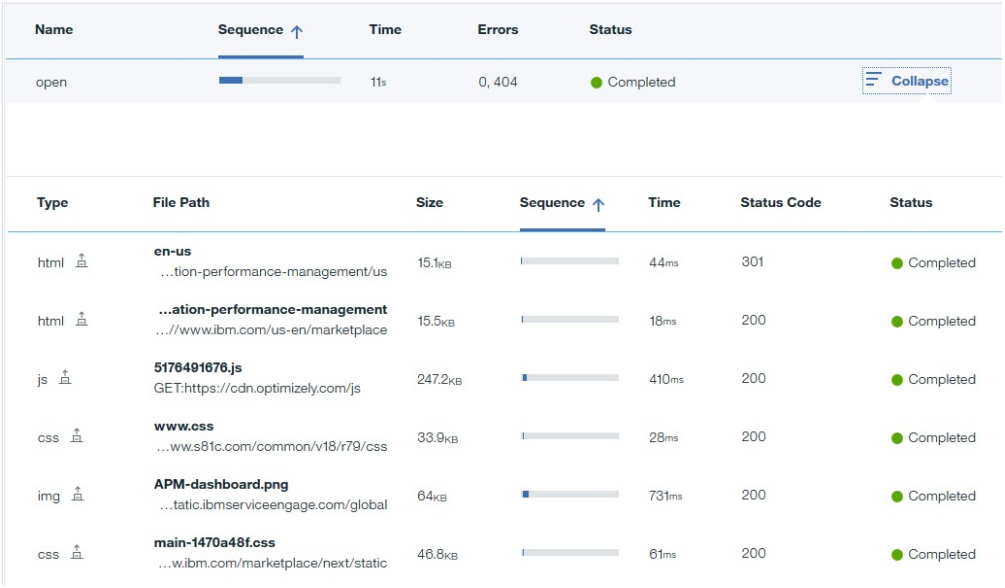


Al pulsar **Expandir** para una instancia de prueba de script, se visualiza el tiempo de respuesta, el número de pasos de script y el número de errores. Para ver los detalles de error, pulse el icono **Información**.

Los siguientes detalles para cada paso de script se muestran en una tabla:

- **Nombre** muestra cada mandato de Selenium al que llama la instancia de prueba, por ejemplo `Open`, `ClickAt` o `VerifyBodyText`.
- **Secuencia** muestra la secuencia de pasos de script desde el principio al final de la instancia de prueba.
- **Tiempo** muestra el tiempo que tarda cada paso de script.
- **Errores** muestra el número de errores que se han producido durante cada paso de script.
- **Estado** describe el resultado del paso de script, por ejemplo, Completado, Desconocido o Anómalo.

Puede descender a mayor nivel de detalle y ver detalles sobre las solicitudes generadas por cada paso de script.



Pulse **Expandir** para ver una tabla que contiene los siguientes detalles:

- **Tipo** muestra el tipo de solicitud, por ejemplo, HTML, CSS, JavaScript o imagen. Las solicitudes externas e internas están representadas por iconos.
- **Vía de acceso de archivo** describe la ubicación del objeto solicitado.
- **Tamaño** muestra el tamaño del objeto solicitado.
- **Secuencia** muestra la secuencia de solicitudes realizadas por la prueba.
- **Tiempo** muestra el tiempo que tarda cada solicitud.
- **Código de estado** muestra el código de estado de solicitud HTTP.
- **Estado** describe el resultado de la solicitud, por ejemplo, Completada, Desconocido o Anómala.

Availability Monitoring puede crear automáticamente una captura de pantalla si la página web no puede cargarse o un paso del script falla. Por ejemplo, si uno de los pasos del script abre una página web pero esta no se carga, Availability Monitoring creará una captura de pantalla automáticamente. Para ver una captura de pantalla de la página web o script, pulse el icono **Error de captura de pantalla** . Esta característica sólo está disponible para pruebas de página web y script. No funciona con las pruebas de API REST.

También puede descargar un registro del tráfico de red para una instancia de prueba determinada como archivo `.har` pulsando el icono **Descargar** . Esta característica está disponible para pruebas de página web y comportamiento programado.

Tiempo de respuesta y disponibilidad

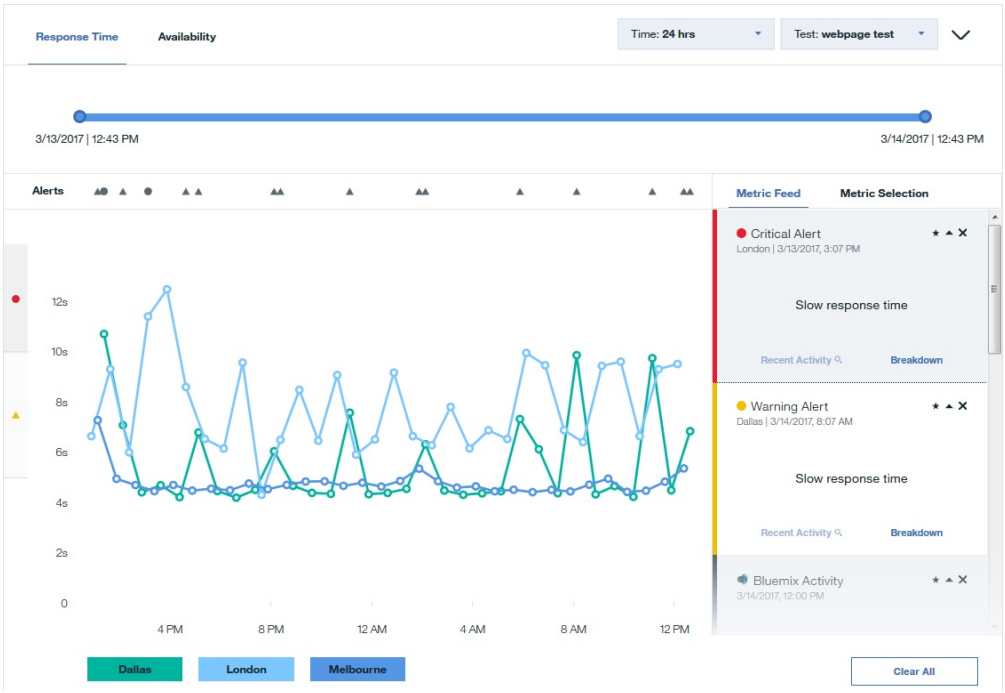
El panel **Tiempo de respuesta y disponibilidad** muestra un gráfico de los tiempos de respuesta medidos y la disponibilidad de las instancias de la prueba durante un periodo definido. Para obtener más información, consulte “Tiempo de respuesta y disponibilidad” en la página 1102.

Tiempo de respuesta y disponibilidad

Utilice el panel **Tiempo de respuesta** y **Disponibilidad** como ayuda para visualizar el tiempo de respuesta, las tendencias de disponibilidad y alertas a lo largo del tiempo.

Gráfico Tiempo de respuesta

La información de tiempo de respuesta se muestra en un gráfico de líneas. Para verlo, pulse el separador **Tiempo de respuesta**.



Importante: Los tiempos de respuesta que se miden mediante Availability Monitoring son ligeramente superiores que los tiempos de respuesta que experimentan los usuarios. Availability Monitoring simula el comportamiento del usuario real, que añade a la medida del tiempo de respuesta. El tiempo de respuesta es mayor debido a los siguientes factores:

- Availability Monitoring crea una instancia de Firefox para cada prueba a fin de evitar que las instancias de prueba anteriores influyan en la prueba actual. Los usuarios reales pueden experimentar tiempos de respuesta más rápidos debido a la memoria caché del navegador.
- Availability Monitoring instala el plug-in controlador web de Firefox antes de cada prueba.

Los tiempos de respuesta individuales para las pruebas están representados por un icono de **Punto de respuesta** en el gráfico de líneas. Los diferentes colores indican las diferentes ubicaciones geográficas en las que se ejecuta la app. El eje Y del gráfico utiliza iconos de alerta para identificar los rangos de umbrales de aviso y críticos. El icono de aviso amarillo representa el rango de umbral de aviso, y el icono crítico rojo representa el rango de umbral crítico. Pulse el icono de aviso amarillo o el icono crítico rojo para identificar fácilmente instancias de prueba que aparecen en los rangos de umbral de aviso y crítico. Para ver los detalles de una instancia de prueba específica, pulse el icono **Icono de respuesta** en el gráfico.

Filtros

Elija una prueba en el menú desplegable **Prueba**. Puede filtrar datos para 3 horas, 24 horas, 7 días, 30 días y 12 meses. Al filtrar para un rango de tiempo superior a 24 horas, los valores que se visualizan en el gráfico son promedios. Para visualizar información más específica, pulse el gráfico para obtener más detalles de los avisos y las alertas individuales. También puede utilizar el control deslizante para ampliar o reducir el intervalo de tiempo.

Con el gráfico de tiempo de respuesta, puede resaltar y ocultar los datos de ubicaciones PoP determinadas. Para resaltar los datos de tiempo de respuesta de una ubicación concreta, pase el cursor por encima del nombre de la ubicación PoP; a continuación, pulse el icono **Resaltar ubicación** . Para ocultar los datos de tiempo de respuesta de una ubicación, pase el cursor por encima

del nombre de la ubicación PoP; a continuación, pulse el icono **Ocultar ubicación**  . Para restaurar datos de ubicación de PoP en el gráfico, pulse **Añadir más ubicaciones** ⊕ o la pestaña **Selección de métrica**; a continuación, pulse la ubicación de PoP que ha eliminado anteriormente.

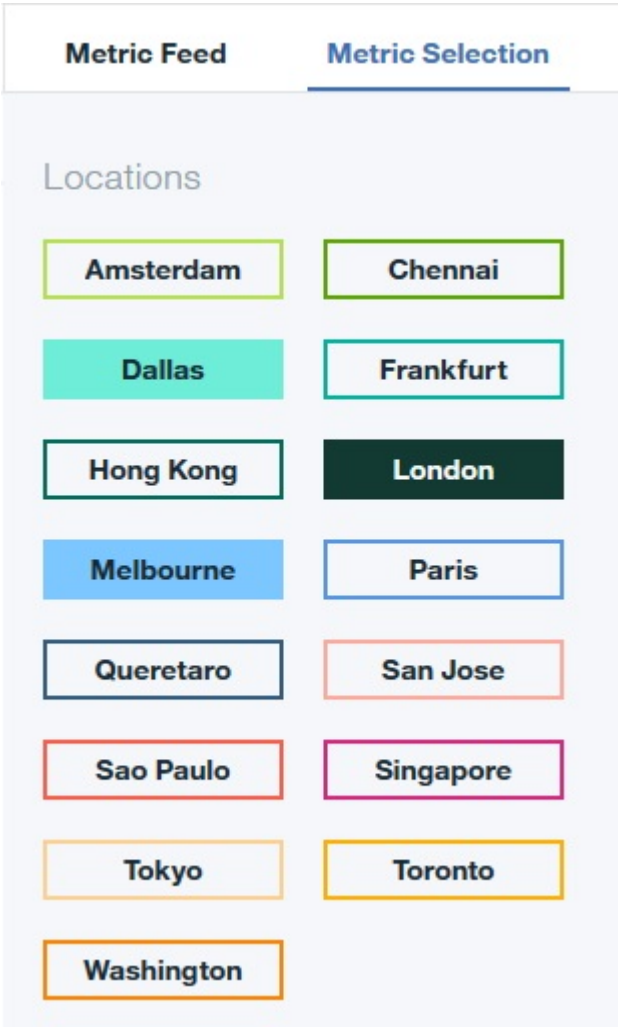
Alertas

Puede identificar fácilmente las alertas de aviso y críticas en la fila Alertas. Pase el ratón por encima de un **icono de alerta** ● ▲ para identificar la gravedad y la indicación de fecha y hora de alerta. Pulse un **icono de alerta** para visualizar los detalles de esa alerta en la **Fuente de datos de métrica**.

Si hay más de un icono cerca en la fila Alertas, un **icono de número** visualiza el número de alertas en ese momento. Pase el puntero del ratón sobre un **icono de número** para visualizar las alertas individuales y pulse una alerta para ver información en la **Fuente de datos de métrica**

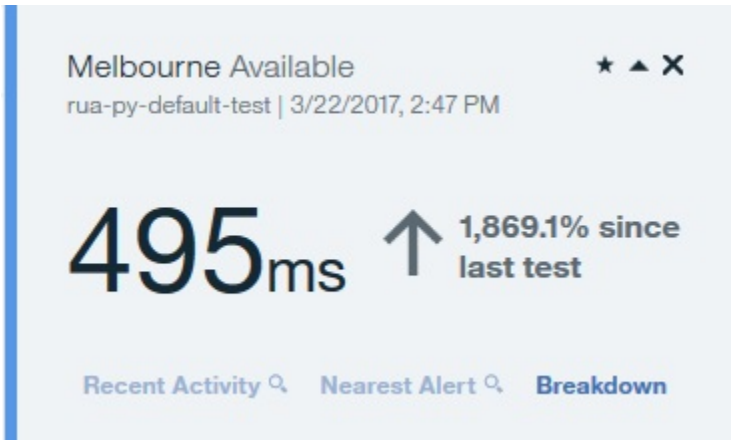
Selección de métrica y Fuente de datos de métrica

Para filtrar por métricas según la región geográfica, pulse **Selección de métrica**. Pulse una ubicación para añadir o eliminar métricas que se miden en esa ubicación del gráfico. Pulse **Añadir más ubicaciones** para abrir la página Modalidad de edición de prueba y añadir una ubicación de PoP a la prueba seleccionada.

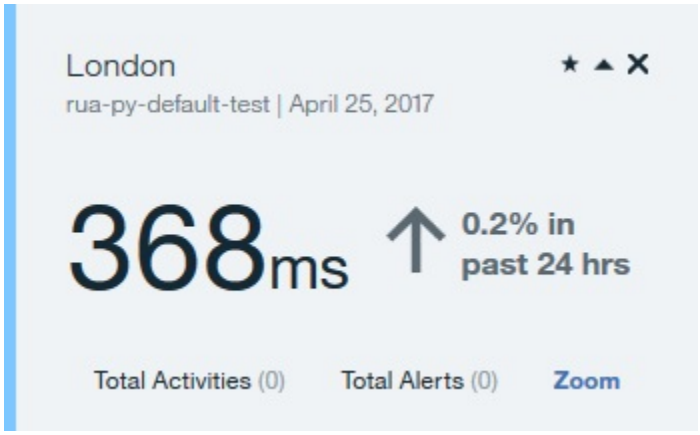


Para ver una lista de detalles de la métrica, pulse **Fuente de datos de métrica**. **Fuente de datos de métrica** muestra una lista de las instancias en las que se satisface una métrica.

Pulse un **icono de alerta** o **punto de respuesta** en el gráfico para añadir los detalles de esa métrica a la **Fuente de datos de métrica**.



Si filtra el gráfico Tiempo de respuesta para un rango de tiempo superior a 24 horas y pulsa un **punto de respuesta**, puede ver detalles agregados para ese día en la **Fuente de datos de métrica**.

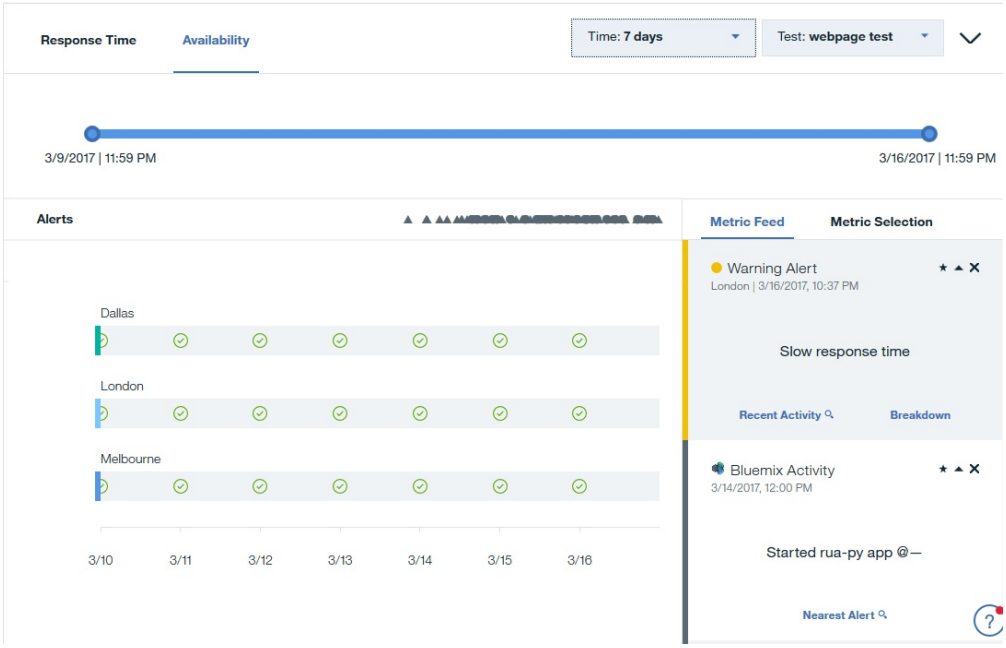


Pulse **Zoom** para ver todos los tiempos de respuesta y alertas generados por la prueba para ese día en el gráfico Tiempo de respuesta.

Para ver información detallada sobre un tiempo de respuesta de alerta o de prueba, pulse **Desglose** en la **Fuente de datos de métrica**. Pulse **Alerta más cercana** para ver la alerta más cercana a esa instancia de prueba en la **Fuente de datos de métrica**, si se ha producido una alerta.

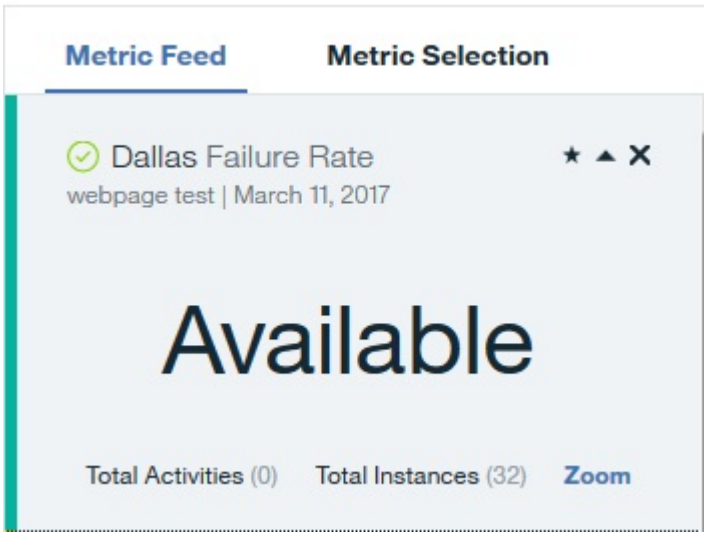
Disponibilidad

Para ver la información de disponibilidad de las aplicaciones, pulse **Disponibilidad**. El gráfico Disponibilidad muestra la disponibilidad diaria de cada punto de presencia (PoP) para la prueba seleccionada.



Con el gráfico de disponibilidad, puede resaltar y ocultar los datos de ubicaciones de PoP determinadas. Para resaltar los datos de disponibilidad de una ubicación concreta, pase el cursor por encima del nombre de la ubicación PoP; a continuación, pulse el icono **Resaltar ubicación**  . Para ocultar los datos de disponibilidad de una ubicación, pase el cursor por encima del nombre de la ubicación PoP; a continuación, pulse el icono **Ocultar ubicación**  . Para restaurar datos de ubicación de PoP en el gráfico, pulse la pestaña **Selección de métrica**; a continuación, pulse la ubicación de PoP que ha eliminado anteriormente.

Pase el ratón por encima de un punto del gráfico para visualizar la tasa de errores y el número de instancias de prueba para un día y ubicación determinados. Pulse un punto del gráfico para visualizar esta información en la **Fuente de datos de métrica**.



Pulse **Zoom** para filtrar el gráfico **Disponibilidad** y el gráfico **Tiempo de respuesta** para visualizar información para el día seleccionado.

Uso de Availability Monitoring

Puede ver detalles sobre el uso de Availability Monitoring en la pestaña **Supervisión** del panel de aplicaciones y en el panel de instrumentos principal de Availability Monitoring.

Para ver una descripción general del uso del panel de instrumentos principal de Availability Monitoring, pulse el icono **Configurar**  . Si es usted un usuario de la versión de prueba de Availability Monitoring, el uso se visualiza como un gráfico de barras y como un porcentaje, conjuntamente con el número de pruebas en uso. Si es usted un usuario del plan prepagado, el uso se visualiza en puntos de datos. Puede ver los detalles de uso para cada prueba individual en el panel **Pruebas sintéticas**.

El uso se mide en puntos de datos. El número estimado de puntos de datos se calcula a partir de la fórmula siguiente:

Número estimado de puntos de datos = T * L * (60/M * 24 * 30) por mes

Donde T = número de pruebas sintéticas ejecutadas, L = número de ubicaciones y M = intervalo entre pruebas (minutos).

Las pruebas simples como por ejemplo las pruebas de página web y de API REST utilizan 1 punto de datos para cada prueba. Las pruebas avanzadas como por ejemplo los scripts de Selenium y los scripts de API REST utilizan 100 puntos de datos para cada prueba.

Exploración de las API

Utilice las API de IBM Cloud Application Performance Management para crear scripts para automatizar la incorporación de su entorno de Cloud APM .Desde la oferta de servicios gestionados por las API de Cloud APM de API Explorer en IBM developerWorks, puede acceder a y explorar las API disponibles de Gestión de grupos de recursos, Servicio de gestión de umbrales y Servicio de control de acceso basado en roles.

Antes de empezar

Debe tener una suscripción a Cloud APM activa para obtener una clave de identificador de cliente y ejecutar operaciones de API.

Procedimiento

1. Abra API Explorer en el navegador: https://developer.ibm.com/api.
2. Inicie sesión con su ID de IBM.
3. En el campo **Buscar en todas las API**, especifique `gestión del rendimiento` y pulse  .
4. Seleccione el recuadro IBM Cloud Application Performance Management API.
5. Pulse **Documentación** en el lado izquierdo de la ventana de API Explorer.
6. Seleccione la API específica.
7. Seleccione la subsección para expandir la lista de operaciones de API.
8. Para continuar, necesita una suscripción a Cloud APM activa. Complete uno de los pasos siguientes:
   a) Si aún no tiene una suscripción a Cloud APM, adquiera una suscripción de prueba gratuita de 30 días.
   b) Si ya tiene una suscripción, inicie la sesión pulsando **Mis API** para probar algunas de las operaciones de API dentro de API Explorer.

   Si la suscripción está activa y ha iniciado la sesión en la página de API Explorer, verá una lista de sus suscripciones de API.
9. Seleccione una operación de API para obtener más detalles.
10. Seleccione uno de los lenguajes (como curl o shell) en la parte superior de la página de API Explorer para ver un ejemplo de solicitud.
11. Recupere su clave de ID de cliente y su clave secreta de cliente y guárdelas en un lugar seguro para uso externo.

    Envíe su clave de ID de cliente y su clave secreta de cliente con cada solicitud de API. Debe tener una suscripción a Cloud APM para completar esta acción.

Qué hacer a continuación
Para obtener más información sobre cómo ejecutar operaciones API, consulte los temas siguientes:

"Acceso y uso de la API Servicio de control de accesos basado en roles" en la página 1045
"Utilización de la API Servicio de gestión de grupos de recursos" en la página 1031
"Utilización de la API del servicio de gestión de umbrales" en la página 1033

Configuración avanzada

Utilice la página **Configuración avanzada** para controlar los valores de las comunicaciones y las funciones avanzadas como, por ejemplo, el reenvío de sucesos.

Después de pulsar **Configuración del sistema** > **Configuración avanzada**, se muestran las siguientes categorías de configuración en la página Configuración avanzada.

Integración de interfaz de usuario
Para productos que se integran con la Consola de Cloud APM, puede añadir o editar el URL para lanzar la aplicación integrada. Los campos se llenan con los URL establecidos durante el procedimiento de configuración de la integración.

- **URL de análisis de registro** se utiliza para lanzar IBM Operations Analytics - Log Analysis para realizar búsquedas en registros de aplicación desde el Panel de instrumentos del rendimiento de aplicaciones. Para obtener más información, consulte "Buscar en archivos de registro" en la página 1115.
- **Habilitar sucesos de subnodo**, para agentes con subnodos, controla si los subnodos se muestran en la pestaña Sucesos. Cuando los sucesos de subnodo están habilitados, se muestran el nodo y subnodo para los que se ha abierto un suceso. Específicamente, si desea visualizar situaciones de supervisión del archivo de registro en la pestaña Sucesos, debe asegurarse de que los sucesos de subnodo están habilitados. Valor predeterminado: `False`.
- **Tasa de renovación de panel de instrumentos** controla la frecuencia de la renovación automática de Panel de instrumentos del rendimiento de aplicaciones. Puede ajustar el valor a cualquier valor de 1 a 60 minutos. El valor afecta al estado de recurso que se visualiza en la pestaña del navegador y la visión general de estado. No tiene ningún efecto en las entradas de la pestaña Sucesos. Valor predeterminado: 1 minuto.

Gestor de sucesos

El gestor de sucesos controla el reenvío de sucesos utilizando Simple Mail Transfer Protocol, así como las notificaciones por correo electrónico. Si especifica un valor para Direcciones de correo electrónico de destino, se enviará un correo electrónico para cada suceso de apertura, cierre y detención. Puede utilizar los campos del **Gestor de sucesos** para configurar los sucesos de Cloud APM para abrir automáticamente incidencias en IBM Control Desk. Para obtener tareas de configuración adicionales, consulte Integración con Control Desk "Integración con Control Desk" en la página 1007.

Si configura el reenviador SMTP para utilizar SSL, debe añadir el certificado de autoridad emisora de certificados de firma del servidor SMTP al almacén de claves del Servidor de Cloud APM. Añada el certificado de autoridad emisora de certificados al almacén de claves predeterminado utilizando el mandato keytool de JVM:

```
dir_instalación/java/jre/bin/keytool -importcert\
-noprompt \
-alias alias_cert_CA \
-file ruta_arch_cert_CA (*.cer)
 -keystore /dir_instalación/wlp/usr/servers/min/resources/security/key.jks \
-storepass ccmR0cKs! \
-storetype jks \
-trustcacerts
```

Para ver un ejemplo de correo electrónico, consulte "Correo electrónico de sucesos" en la página 1110.

- **Direcciones de correo electrónico de destino** especifica las direcciones de correo electrónico a los que se reenvían los sucesos. Separe cada dirección con una coma (,), por ejemplo, `annette@ibm.com,jim@ibm.com,owen@ibm.com`.
- **Alert Notification para ITMv6** es la opción para habilitar Alert Notification para sucesos ITMv6 estableciendo el valor en `True`. Valor predeterminado: `False`
- **Cloud Event Management Webhook** es el URL de Webhook que se genera en Cloud Event Management cuando se configura la integración entre IBM Cloud Application Performance Management y Cloud Event Management. Debe pegar aquí el URL de Webhook generado para que los sucesos se reenvíen desde Cloud APM.

Puede utilizar Alert Notification en lugar de la función de correo electrónico del Gestor de sucesos, que le permite controlar quién ha avisado de los distintos sucesos y cómo se han notificado. Para obtener más información, consulte "Integración con Alert Notification" en la página 1005.

Si está reenviando sucesos a un receptor EIF (recurso de integración de sucesos), puede personalizar los atributos EIF, por ejemplo, para añadir un atributo al suceso de EIF. Para obtener más información, consulte el apartado "Personalización de un suceso para reenviarlo a un receptor EIF" en la página 1025. Para obtener información sobre cómo reenviar los sucesos al gestor de sucesos de IBM Netcool/OMNIbus, consulte el tema de "Integración con Netcool/OMNIbus" en la página 999.

Servicio de herramientas de análisis de rastreo

Los valores utilizados para el servicio de herramientas de análisis de rastreo. Los valores se aplican solo a la oferta Cloud APM, Advanced y si está configurando el rastreo de transacciones en el entorno.

- **Tamaño de la agrupación de conexiones** es el número de conexiones Db2 simultáneas que mantiene el servicio de herramientas de análisis de rastreo en la agrupación de conexiones para la consulta "Top*N*". Aumente este valor si experimenta tiempos de consulta lentos debido a un gran número de usuarios simultáneos de la Consola de Cloud APM Valor predeterminado: `10`.
- Los **Pseudonodos** permiten la visualización de servicios que no están instrumentos. Valor predeterminado: `True`.
- **Tiempo de espera de consulta en segundos** es el número de segundos que utiliza cada consulta "Top*N*" (donde *N* es un número, como en "Top 5" o "Top 10") antes de exceder el tiempo de espera. Si se requiere, se puede aumentar el valor de tiempo de espera para las aplicaciones con una mayor carga de trabajo y cuyos tiempos de se espera que sean más largos. Valor predeterminado: `120` segundos.
- No suele ser necesario cambiar **Reoptimización de consulta DB2 habilitado**. El parámetro afecta al optimizador de consultas de Db2. En algunos entornos, si se desactiva el optimizador podría mejorar el rendimiento de algunos conjuntos de transacciones. Valor predeterminado: `False`.

Recurso de suscripción de agente

El Recurso de suscripción de agente incluye la interfaz de agente REST (Representative State Transfer) y el servidor HTTP de Servicios de configuración central. La interfaz REST la utilizan los agentes y los recopiladores de datos para enviar datos de supervisión que persisten en el servidor de Db2 y los sucesos de umbral. El servidor HTTP de Servicios de configuración central maneja solicitudes de agentes para sus archivos de configuración, por ejemplo, definiciones de umbral. Utilice estos parámetros para configurar las comunicaciones entre el Recurso de suscripción de agente y el Servidor de Cloud APM.

- **Límite de sondeo omitido (pulsación rápida)** es el número máximo de veces que un agente de supervisión con un intervalo de latidos de 60 segundos o menos no se conecta antes de que se marque fuera de línea. Valor predeterminado: `30` intervalos.
- **Límite de sondeo omitido (pulsación lenta)** es el número máximo de veces que un agente de supervisión con un intervalo de latidos mayor de 60 segundos no se conecta antes de que se marque fuera de línea. Valor predeterminado: 3 intervalos.
- **Tiempo de espera de transacción** es el tiempo, en segundos, que el servidor espera una respuesta a una solicitud. Valor predeterminado: `120` segundos.
- **Eliminar retardo de sistema fuera de línea** determina el número de minutos que hay que esperar antes de eliminar la visualización de un sistema gestionado fuera de línea. En el Panel de

instrumentos del rendimiento de aplicaciones, los sistemas gestionados fuera de línea se indican mediante el indicador de estado desconocido . El sistema gestionado sigue visualizándose, incluso cuando se desinstala el agente, hasta que pasa el tiempo de retardo. Para obtener más información, consulte "Visualización y eliminación de agentes fuera de línea" en la página 1138. Valor predeterminado: 5760 minutos (4 días).

Habilitación de umbrales

Cada agente de supervisión viene con un conjunto de umbrales predefinidos que están habilitados y se inician con el agente. Estos umbrales predefinidos están asignados al grupo de recursos del sistema por omisión para el agente.

- **Eligir una acción para definir la política para umbrales de mejores usos predefinidos** controla si los umbrales predefinidos para sus recursos gestionados están habilitados o inhabilitados de forma predeterminada. Establezca el campo en **Inhabilitar todos** si no desea ejecutar los umbrales predefinidos. El valor **Inhabilitar todos** elimina la asignación del grupo de sistemas de todos los umbrales predefinidos. Un umbral sin ningún grupo asignado no se distribuye a ningún sistema supervisado y permanece detenido hasta que se distribuye a un grupo de recursos. Si decide posteriormente que desea activar los umbrales predefinidos, establezca el campo en **Habilitar todos**.

Para obtener más información sobre los umbrales predefinidos y los umbrales personalizados, consulte "Información básica" en la página 1010 y "Ejemplos de umbrales inhabilitados" en la página 1012.

Correo electrónico de sucesos

Utilice los campos del Gestor de sucesos en la página Configuración avanzada para configurar la notificación de sucesos por correo electrónico a una lista de direcciones.

Correo electrónico de suceso abierto

Cuando se cumple una condición de umbral, se abre un suceso y el mensaje de correo electrónico enviado por el Servidor de Cloud APM contiene los atributos base aplicables a todos los sucesos + atributos de agente de la primera fila del conjunto de datos que coinciden con la condición de umbral. El atributo situation_status tiene el valor Y para los sucesos abiertos.

Correo electrónico de suceso de cierre

Cuando la condición de umbral ya no se cumple, se genera un suceso de cierre. El mensaje de correo electrónico de los sucesos de cierre sólo contiene los atributos base aplicables a todos los sucesos de agente y el valor de situation_status es N. Los atributos del agente no se incluyen en estos mensajes de correo electrónico porque la condición de umbral no se cumple.

Correo electrónico de suceso de detención

Cuando se detiene un umbral, se genera un suceso de detención. El mensaje de correo electrónico de los sucesos de detención sólo contiene los atributos base aplicables a todos los sucesos de agente y el valor de situation_status es P. Los atributos del agente no se incluyen en estos mensajes de correo electrónico porque la condición de umbral no se cumple.

Un umbral se detiene para un agente si se suprime la definición de umbral o se realiza un cambio en cualquiera de las definiciones de umbral que se distribuyen al agente.

Los ejemplos siguientes muestran un correo electrónico para un suceso abierto:

```
De:    noreply@apm.ibmserviceengage.com
A:         tester@us.ibm.com
Fecha:    10/25/2017 01:56 PM
Asunto:    Linux_Disk_Space_Low on nc049048:LZ (Notification)
El texto siguiente muestra la información recibida del agente que desencadenó este suceso.
Los valores IP y Agente identifican el agente que ha detectado el suceso.
Los valores Descripción y Gravedad especifican el nombre de la definición de umbral y su
gravedad.
Debajo de la Descripción se encuentran todos los pares atributo/valor
existentes en el suceso, en su formato original.
    IP servidor: 10.107.76.230 (SIDR26APAP1BLUE.test.ibm.com)
    IP agente  : 9.42.49.48
    Agente     : nc049048:LZ
    Gravedad   : warning
    Descripción: Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10
```

```
                AND FS_Type != nfs  AND FS_Type != iso9660 ]
      ITM_KLZ_Disk
      ManagedSystemGroups='*LINUX_SYSTEM'
      TenantID=F43E-D704-DADC-6270-1ED8-543E-A388-6513
      adapter_host=nc049048.tivlab.raleigh.ibm.com
      apm_hostname=SIDR26APAP1BLUE.test.ibm.com
      appl_label=A:P:S
      date=01/25/2017
      disk_free=5843
      disk_free_percent=20
      disk_name=/dev/sda2
      disk_used=22676
      disk_used_percent=80
      file_system_status=2
      file_system_status_enum=Up
      fqhostname=nc049048.test.ibm.com
      fs_type=ext4
      hostname=nc049048.test.ibm.com
      identifier=Linux_Disk_Space_Lownc049048:LZ/ITM_KLZ_Disk
      inodes_free=1721587
      inodes_free_percent=88
      inodes_used=232477
      inodes_used_percent=12
      integration_type=U
      mount_options=rw
      mount_point=/
      msg='Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10  AND FS_Type !
= nfs
     AND FS_Type != iso9660 ]'
      origin=9.42.49.48
      severity=WARNING
      situation_displayitem=/
      situation_eventdata='disk_name=/dev/
sda2;inodes_used_percent=12;mount_options=rw;fs_type=ext4;

system_name=nc049048:LZ;mount_point=/;disk_used_percent=80;disk_free=5843;file_system_status_enum=
Up;
     size=30040;disk_used=22676;inodes_used=232477;disk_free_percent=20;file_system_status=2;
     total_inodes=1954064;inodes_free=1721587;timestamp=1170125135553000;inodes_free_percent=88;~'
      situation_name=Linux_Disk_Space_Low
      situation_origin=nc049048:LZ
      situation_origin_uuid=09fb36afd6b3.22.02.09.2a.31.30.56.9d
      situation_status=Y
      situation_thrunode=nc049048:LZ
      situation_time='01/25/2017 13:55:55.000'
      situation_type=S
      size=30040
      source='ITM Agent: Private Situation'
      sub_origin=/
      sub_source=nc049048:LZ
      system_name=nc049048:LZ
      timestamp=1170125135553000
      tmz_diff=18000
      total_inodes=1954064
Para anular la suscripción a estos correos electrónicos: inicie sesión en la consola de Cloud APM
y elimine su dirección de correo electrónico de la lista de direcciones de correo electrónico de
la
categoría Gestor de sucesos de la página Configuración avanzada.
```

El ejemplo siguiente muestra un correo electrónico para un suceso de cierre.

```
De:    noreply@apm.ibmserviceengage.com
A:         tester@us.ibm.com
Fecha:   01/25/2017 02:01 PM
Asunto:    Linux_Disk_Space_Low on nc049048:LZ (Closed)
El texto siguiente muestra la información recibida del agente que desencadenó este suceso.
Los valores IP y Agente identifican el agente que ha detectado el suceso.
Los valores Descripción y Gravedad especifican el nombre de la definición de umbral y su
gravedad.
Debajo de la Descripción se encuentran todos los pares atributo/valor existentes en el
suceso en su formato original.
    IP servidor: 10.107.76.230 (SIDR26APAP1BLUE-12f.test.ibm.com)
    IP agente  : 9.42.49.48
    Agente     : nc049048:LZ
    Gravedad   : warning
    Descripción: Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10
                 AND FS_Type != nfs  AND FS_Type != iso9660 ]
      ITM_KLZ_Disk
      ManagedSystemGroups='*LINUX_SYSTEM'
      TenantID=F43E-D704-DADC-6270-1ED8-543E-A388-6513
      adapter_host=nc049048.tivlab.raleigh.ibm.com
      apm_hostname=SIDR26APAP1BLUE-12f.test.ibm.com
```

```
      appl_label=A:P:S
      date=01/25/2017
      fqhostname=nc049048.test.ibm.com
      hostname=nc049048.test.ibm.com
      identifier=Linux_Disk_Space_Lownc049048:LZ/ITM_KLZ_Disk
      integration_type=U
      msg='Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10  AND FS_Type !
= nfs
     AND FS_Type != iso9660 ]'
      origin=9.42.49.48
      severity=WARNING
      situation_displayitem=/
      situation_eventdata=~
      situation_name=Linux_Disk_Space_Low
      situation_origin=nc049048:LZ
      situation_origin_uuid=09fb36afd6b3.22.02.09.2a.31.30.56.9d
      situation_status=N
      situation_thrunode=nc049048:LZ
      situation_time='01/25/2017 14:00:55.000'
      situation_type=S
      source='ITM Agent: Private Situation'
      sub_origin=/
      sub_source=nc049048:LZ
      tmz_diff=18000
Para anular la suscripción a estos correos electrónicos: inicie sesión en la consola de Cloud APM
y elimine su dirección de correo electrónico de la lista de direcciones de correo electrónico de
la
categoría Gestor de sucesos de la página Configuración avanzada.
```

Capítulo 10. Utilización de los paneles de instrumentos

Seleccione **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** para obtener una visión general global del estado de las aplicaciones. Puede obtener más información, desde una visión general de alto nivel a métricas detalladas en la misma pantalla.

Utilice las herramientas que están disponibles en los paneles de instrumentos para investigar condiciones críticas y de aviso en el entorno, crear vistas de métricas adicionales y para realizar acciones como buscar registros de rastreo y comparar métricas a lo largo del tiempo.

Todas mis aplicaciones – Panel de instrumentos del rendimiento de aplicaciones

Panel de instrumentos del rendimiento de aplicaciones presenta el estado de resumen de los dominios supervisados en **Todas mis aplicaciones**. Se visualiza un *cuadro de resumen* para cada aplicación definida por el usuario, como "Gestión de inventario" y para las aplicaciones predefinidas, "Mis componentes" o "Mis transacciones" si el entorno las incluye. Desde los cuadros de resumen o desde el navegador aumente el nivel de detalle de cada aplicación y de sus componentes para ver métricas detalladas.

A medida que selecciona elementos, se muestra la vía de acceso y puede pulsar uno de los enlaces de vía de acceso para volver a dicha vista. En cualquier página de la Consola de Cloud APM, puede pulsar **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** para abrir el panel de instrumentos **Todas mis aplicaciones**. Vea las áreas de interés seleccionando del navegador o pulsando en un cuadro de resumen para avanzar al nivel siguiente.

Cuadros de resumen

Todas mis aplicaciones tiene un cuadro de resumen de cada aplicación definida. Los indicadores muestran la gravedad de estado más elevada para la aplicación en la barra de título y para cada grupo en el cuadro de resumen. Están disponibles los siguientes grupos predefinidos, en función de qué productos de supervisión están incluidos en la aplicación definida:

- **Availability Monitoring** no tiene subgrupos
- **Componentes** tiene un subgrupo por cada tipo de agente de supervisión que soporta su aplicación
- **Transacciones** puede incluir los subgrupos **Transacciones de usuario final** y **Transacciones sintéticas** (IBM Website Monitoring on Cloud antes del release de agosto de 2017)

Además, cada cuadro de resumen incluye **Sucesos**, que muestra la gravedad del suceso de gravedad más elevada que se ha abierto para la aplicación. Puede pulsar el enlace Sucesos para investigar los sucesos abiertos (consulte “Estado de suceso” en la página 1143).

 Pulse una barra de título de cuadro de resumen para abrir la pestaña Visión general de estado para la aplicación. O pulse uno de los iconos del cuadro de resumen para abrir la pestaña Visión general de estado para el grupo Componentes o el subgrupo Usuarios o Transacciones, o para abrir la pestaña Sucesos para el grupo o subgrupo de aplicación.

Puede contraer los cuadros de resumen y filtrarlos seleccionando o deseleccionando los recuadros de selección:

- Para mostrar sólo las barras de título del cuadro de resumen para facilidad de desplazamiento a través de las aplicaciones definidas, deseleccione el recuadro de selección **Mostrar detalles**.
- Para filtrar los recuadros de resumen para el estado de gravedad que desea ocultar, desmarque el recuadro de selección para un contador como, por ejemplo,  . El recuadro de selección de

una gravedad sin sucesos está inhabilitado. Por ejemplo, en este gráfico, los filtros para Crítico y Normal están habilitados; Aviso y Desconocido están inhabilitados porque tienen un recuento de 0:  .

Buscar

El campo Buscar se utiliza para encontrar entradas de registro de la hora anterior que contienen el texto especificado. Puede pulsar  para mostrar los resultados de un rango horario distinto. El texto de la búsqueda se compara con las entradas de registro asociadas a la selección de navegador y las posibles coincidencias se muestran en una nueva pestaña o ventana de navegador. Encontrará instrucciones en: "Buscar en archivos de registro" en la página 1115. La función de búsqueda se proporciona mediante IBM Operations Analytics - Log Analysis.

Acciones

El menú **Acciones** tiene opciones para copiar el URLabriendo el registro del panel de instrumentos y para establecer un rastreo para la resolución de problemas. Si desea más información, consulte "Copia del URL del panel de instrumentos" en la página 1156 y "Configuración de un rastreo" en la página 1157.

Utilice la opción **Registro del panel de instrumentos** para revisar la lista de paneles de instrumentos del agente que se han actualizado desde el último reinicio del servidor.

Cuando está seleccionado el panel de instrumentos inicial **Todas mis aplicaciones** o una de las aplicaciones, el menú Acciones incluye **Lanzar a informes** para ayudarle a analizar las tendencias de uso y de rendimiento si los informes basados en Cognos están disponibles y su entorno incluye Tivoli Common Reporting. Para obtener más información, consulte "Informes" en la página 1158.

Cuando el grupo **Componentes** está seleccionado, desde la sección **Grupos** del navegador o desde un cuadro de resumen, el menú **Acciones** incluye una opción **Editar** para editar el panel de instrumentos Visión general de estado de componentes. La opción **Editar** sólo está disponible si el usuario que ha iniciado sesión tiene el permiso Modificar para el panel de instrumentos de Performance Management y el permiso Crear para Aplicaciones. Para obtener más información, consulte "Edición de los widgets del grupo del panel de instrumentos Componentes" en la página 1124.

Ayuda

Abra la ayuda emergente para obtener una descripción breve del panel de instrumentos actual, con los enlaces siguientes: **Más información** abre el tema del panel de instrumentos completo en el sistema de ayuda de Cloud APM local; y **Realizar una visita guiada del panel de instrumentos** inicia la visita guiada del panel de instrumentos de IBM Cloud APM, que presenta una descripción breve de los elementos del panel de instrumentos mientras le guía a través de las características.

Navigator

El navegador muestra una jerarquía de las aplicaciones definidas y de sus usuarios, transacciones y componentes, que muestra cómo están organizados. El navegador tiene una sección por cada nivel de la jerarquía de aplicaciones. En cada nivel del navegador, las métricas del panel de instrumentos cambian para mostrar los datos del componente. Seleccione un elemento para cambiar el contexto del panel de instrumentos al de la selección. El ámbito de lo que puede ver está determinado por sus permisos de usuario.

Cada elemento de navegador tiene un indicador de estado  crítico,  aviso, normal o  desconocido, que indica que el agente no está disponible. Cada sección de navegador presenta un recuento de sucesos para cada gravedad asociada al elemento de Navigator seleccionado. Para una correlación de estado a sucesos de umbral, consulte "Estado de suceso" en la página 1143.

Para crear más espacio para otras secciones, pulse una barra de título para contraer la sección y vuelva a pulsarla para restaurarla. También puede ocultar el navegador por completo pulsando en el borde del navegador; y restaurarlo pulsando , o ajustar el ancho arrastrando el borde .

El navegador tiene tres secciones:

- La sección **Aplicaciones** lista todas las aplicaciones definidas en los dominios o que están permitidas para el rol de usuario.

  - Una vez seleccionada la aplicación, el panel de instrumentos cambia a un resumen de estado de alto nivel en la pestaña **Descripción general de estados** y se muestra un indicador del estado de gravedad más alta en la pestaña **Sucesos**. Para obtener más información, consulte "Aplicación – Panel de instrumentos del rendimiento de aplicaciones" en la página 1116.
  - Los componentes del dominio que han sido descubiertos por la infraestructura de supervisión se muestran en la aplicación predefinida denominada "Mis componentes", que no se puede editar ni suprimir.
  - Si tiene privilegios de rol de administrador, la barra de herramientas **Aplicaciones** incluye las herramienta  para gestionar aplicaciones. Para obtener instrucciones, consulte "Gestión de aplicaciones" en la página 1133.
- Después de seleccionar una aplicación, la sección **Grupos** muestra los grupos que dan soporte a la aplicación. Para obtener más información, consulte "Grupo e instancia – Panel de instrumentos del rendimiento de aplicaciones" en la página 1121.
- Después de seleccionar su subgrupo, la sección **Instancias** se redenomina para el título de subgrupo y se llena con los nombres de sistema gestionado individuales. La **Visión general de estado** cambia para mostrar los ICR para el subgrupo seleccionado. Después de seleccionar un sistema gestionado, se visualizan widgets de grupo detallados con los ICR del sistema gestionado. Para instancias de componente también tiene una pestaña **Detalles de atributo** para ver una tabla de ICR de los atributos de conjunto de datos de su elección. Para obtener más información, consulte "Visualización y gestión de gráficos y tablas personalizados" en la página 1127.

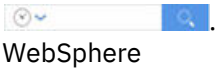
Si obtiene un mensaje emergente **Error de red** en el navegador, los indicadores de estado pueden cambiar a  normal hasta después de que se restaure la conexión. En cualquier momento, se vuelven a procesar todos los sucesos abiertos y el estado puede aparecer normal hasta que se completa el proceso.

Buscar en archivos de registro

Para encontrar la causa raíz de un problema experimentado por usuarios como, por ejemplo, lentitud o una anomalía, puede buscar en los datos de registro asociados a las aplicaciones. IBM Operations Analytics - Log Analysis proporciona la prestación de búsqueda. Los datos de registro de aplicación y los datos de rendimientos se unen para ayudarle a encontrar la causa raíz de un problema experimentado por las aplicaciones y acelerar la resolución del problema.

Procedimiento

Realice los pasos siguientes para localizar las entradas de registro que podrían estar correlacionadas con un problema que está investigando, como un uso elevado de la CPU.

1. Si no se muestra el Panel de instrumentos del rendimiento de aplicaciones, selecciónelo en el menú  **Rendimiento**.
2. Si desea buscar dentro de una aplicación, seleccione una de las aplicaciones en el panel de instrumentos "Todas mis aplicaciones".
   Por ejemplo, pulse "Mis componentes" para buscar en los registro de todos los recursos de componente.
3. Escriba el texto del archivo de registro para encontrar en el recuadro de búsqueda  .
   Por ejemplo, especifique `retrotraído` para buscar en los recursos de Agente de WebSphere Applications que se han retrotraído al nivel anterior.
4. Si desea encontrar datos dentro de un rango de tiempo distinto a **Última hora**, pulse  y seleccione un periodo de tiempo.
5. Pulse  .

Resultados

Todas las entradas de registro que contienen el texto de búsqueda en el contexto del nivel del navegador actual se visualizan en una pestaña o ventana nueva del navegador. La ventana de navegador se denominada con respecto al contexto como, por ejemplo, la aplicación "Proceso de tarjeta de crédito".

Qué hacer a continuación
Revise los resultados de la búsqueda. Puede seleccionar otra aplicación para cambiar los resultados de búsqueda para el contexto. Utilice el campo de búsqueda para refinar más los resultados. Por ejemplo, si el campo de búsqueda muestra `db2 AND (datasourceHostName:Pear* OR datasourceHostname:Persimmon* OR datasourceHostname:Pomegranate*)`, puede suprimir orígenes de datos para acotar los resultados: `db2 AND (datasourceHostname:Persimmon*)`.

Para obtener más información, consulte la recopilación de temas de IBMOperations Analytics Log Analysis en el IBM Knowledge Center o vaya a IBM Operations Analytics - Developers Community.

Aplicación – Panel de instrumentos del rendimiento de aplicaciones

Después de seleccionar una aplicación desde el navegador o desde un recuadro de resumen del panel de instrumentos **Todas mis aplicaciones**, un panel de instrumentos con pestañas presentará distintas facetas de su aplicación. La pestaña **Descripción general de estados** presenta un resumen de estados de alto nivel de su aplicación. Los umbrales de gráfico y los indicadores de estado proporcionan información general sobre el estado y el rendimiento. Seleccione la pestaña **Sucesos** para ver qué umbrales de suceso contribuyen a la salud de la aplicación.

ara ver una descripción de los elementos del navegador y banner, consulte “Navigator” en la página 1114, “Buscar” en la página 1114, “Acciones” en la página 1114 y “ Ayuda” en la página 1114.

Visión general de estado

- Dependiendo de la composición de la aplicación seleccionada, la pestaña **Visión general de estado** presenta una o más perspectivas para evaluar el estado de la aplicación a un nivel alto:

  Disponibilidad a lo largo del tiempo
  IBM Website Monitoring on Cloud antes del release de agosto de 2017: El gráfico de barras **Disponibilidad a lo largo del tiempo** se visualiza si la aplicación incluye el Agente de Synthetic Playback (en el grupo de navegador **Transacciones** y en la aplicación predefinida **Mis transacciones**).

  Cada punto de gráfico es un ejemplo de transacción con un indicador de color para un estado de **Buen estado**, **Lento** o **No disponible**.

  Pulse en cualquier parte de la línea de tiempo de la barra para abrir una ventana emergente con las tablas **Lista de transacciones** y **Lista de ubicaciones**.

  Solicitudes y tiempo de respuesta
  El gráfico de barras apiladas **Solicitudes y tiempo de respuesta** se visualiza si la aplicación incluye el Agente de Supervisión de tiempo de respuesta (**Transacciones de usuario final** en el grupo de navegador **Transacciones**).

  Este gráfico se utiliza para buscar patrones de tendencia en el rendimiento. Cada barra apilada representa el porcentaje de peticiones completadas con tiempos de respuesta bueno, lento o que no se han completado. La superposición de gráfico de líneas representa el tiempo medio de respuesta durante el período de 5 minutos. Utilice el selector de tiempo para cambiar el intervalo de tiempo mostrado, que se describe en “Ajuste y comparación de métricas a lo largo del tiempo” en la página 1125.

  Topología de transacciones agregada
  La **Topología de transacciones agregada** se visualiza cuando el rastreo de transacciones está habilitado y la aplicación incluye cualquiera de los agentes o recopiladores de datos siguientes:

  - Agente de DataPower
  - Agente de HTTP Server
  - Agente de IBM Integration Bus
  - Recopilador de datos de J2SE
  - Agente de JBoss

- Recopilador de datos de Liberty
- Agente de Microsoft .NET
- Agente de Microsoft SQL Server
- Recopilador de datos de Node.js
- Agente de Supervisión de tiempo de respuesta
- Agente de SAP NetWeaver Java Stack
- Agente de Tomcat
- Agente de WebLogic (solo Linux y Windows)
- Agente de WebSphere Applications
- Agente de WebSphere MQ

Debe habilitar el rastreo de transacciones manualmente para todos los agentes, salvo el Agente de Supervisión de tiempo de respuesta. El rastreo de transacciones está habilitado automáticamente para recopiladores de datos. Para obtener más información, consulte "Página Configuración de agente" en la página 189.

La **Topología de transacciones agregada** presenta los recursos que están asociados con la aplicación y sus relaciones. El pie de página muestra un recuento de los nodos, recursos, relaciones y filtros seleccionados en la topología, así como la hora cuando los datos se renovaron por última vez.

Si un componente de la aplicación se añade a una aplicación empresarial, y el componente lleva tráfico para varias aplicaciones, la topología de la aplicación que se muestra para estas aplicaciones empresariales incluye vías de acceso a nodos para todas las aplicaciones.

Para la Pila de aplicaciones Java de IBM donde JavaScript se inyecta automáticamente, el nodo de nivel más elevado representa el navegador, y el nodo más granular es la base de datos. Para otras aplicaciones, el nodo de nivel más elevado representa la aplicación y el nodo más granular es la instancia de sistema gestionado.

Cada nodo tiene un indicador de estado y un resaltado de fondo para mostrar la gravedad de estado más alta a ese nivel de agregación. Si contrae el navegador para dejar más espacio, puede seguir viendo el mismo estado en la **Topología de transacciones agregada**. El entorno de origen del nodo se muestra como **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **Local** (IBM Cloud Application Performance Management, Private) , **Nube privada** (IBM Cloud Private) o **Nube pública** (IBM Cloud). No se muestra ningún icono **Otros** (el recurso gestionado es de otro entorno).

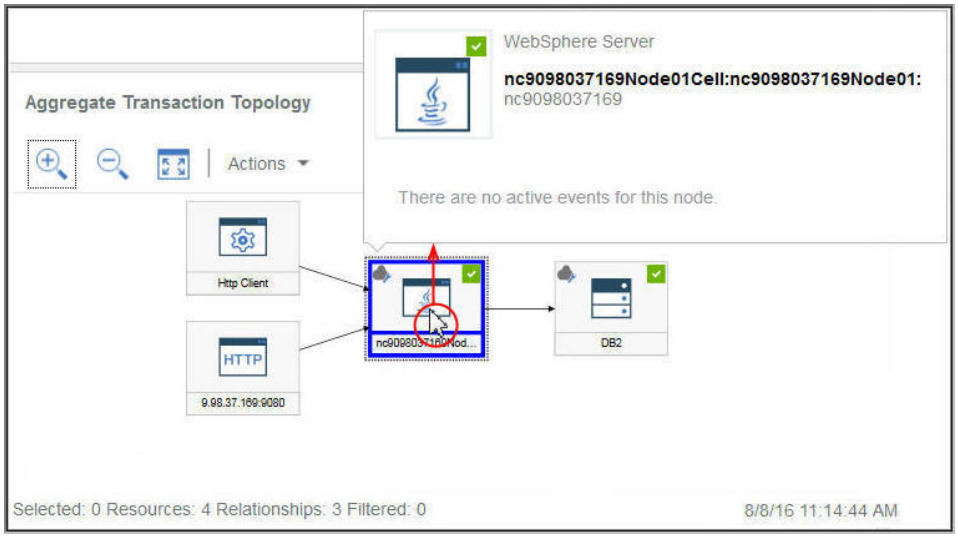
Pase el ratón sobre un nodo, abra el menú contextual y seleccione los nodos para obtener más información sobre el estado y como ayuda para identificar la causa raíz de un problema:

- Cuando pasa el cursor por encima de un nodo, un mensaje emergente proporciona una lista de los sucesos críticos y de aviso.
- Efectúe una doble pulsación sobre un URL de enlace en un nodo para abrir el panel de instrumentos correspondiente con detalles de componente o de transacción.
- Pulse el botón derecho del ratón en un nodo y seleccione una de las opciones de detalle del panel de instrumentos: **Ir a la página Resumen de transacciones** del nodo de subgrupo seleccionado; **Ir a la página Instancia de componente** del nodo de la instancia; o **Propiedades** para ver el nombre del recurso, el estado, el nombre del sistema gestionado y el dominio de proveedor (como "Nube").

Utilice los iconos de la barra de herramientas para ajustar la visualización y realizar acciones tal como se describe en "Manipulación del widget Topología de transacciones agregada" en la página 1120.

Pulse la herramienta para alternar entre esta vista y el **Estado de componentes actuales**, descrito aquí.

Los agentes de supervisión sin información de topología no se muestran en el widget de Topología de transacciones agregada.



Estado actual de componentes

El gráfico de barras apiladas **Estado actual de componentes** muestra el porcentaje y un recuento de estados críticos, de aviso, normales y desconocidos de cada tipo de componente de la aplicación. Suponga, por ejemplo, que 5 sistemas Linux soportan la aplicación seleccionada. Una barra apilada que muestre 40% crítico y 60% normal indica que 2 sistemas tienen estado crítico y 3 sistemas tienen estado normal.

Pase el puntero del ratón sobre un segmento de barra para leer el estado en una ventana emergente: el porcentaje y el recuento de las instancias del componente con ese estado. El dominio o dominios donde residen las instancias también se muestra con un recuento de estado para cada dominio: IBM Cloud, en la nube, local, ITM y otros. Por ejemplo, 2 de sus 5 sistemas Linux están en el dominio de ITM y 3 están en el dominio de la nube. Si uno de los sistemas críticos está en el dominio de ITM y el otro está en dominio de la nube, cuando pase el cursor del ratón por encima del segmento de barra Crítico 40%, la ventana emergente de estado mostrará 1 sistema en el dominio de ITM y 1 en el dominio de la nube.

Puede pulsar una barra para abrir el panel de instrumentos de resumen de estado del tipo de componente, con un widget de grupo por cada sistema supervisado.

Pulse la herramienta ⊖ para conmutar entre esta vista y la **Topología de transacción de agregado**, se ha descrito anteriormente.

Availability Monitoring

Cuando la aplicación consta solo de Availability Monitoring, el panel de instrumentos de resumen se visualiza tal como se describe en "Acceso a Availability Monitoring" en la página 1082.

- Después de seleccionar un subgrupo en la sección **Grupos**, la sección **Instancias** se redenomina para el título de subgrupo y se llena con los nombres de instancia individuales. Para obtener información sobre los paneles de instrumentos a nivel de grupo, subgrupo e instancia del navegador, y sobre la pestaña **Detalles de atributo** que se abre después de seleccionar un sistema gestionado, consulte "Grupo e instancia – Panel de instrumentos del rendimiento de aplicaciones" en la página 1121 y "Visualización y gestión de gráficos y tablas personalizados" en la página 1127.
- Algunos de los widgets del panel de instrumentos muestran métricas que se basan en un rango de tiempo, y otros widgets muestran las métricas más recientes. Si se muestra una barra de selección de tiempo, puede ajustar el periodo de tiempo del panel de instrumentos que afecta a los gráficos o a las tablas cuyos valores se derivan de las muestras de datos históricas. Para obtener más información, consulte "Ajuste y comparación de métricas a lo largo del tiempo" en la página 1125.
  Mientras visualiza gráficos, puede pulsar un punto de gráfico para abrir una ayuda contextual con el valor del punto de gráfico y demás información pertinente. Después de visualizar un gráfico de líneas en el navegador Internet Explorer Versión 11, quizá siga viendo la ayuda contextual mientras mueve el

cursor alrededor de la ventana. Si experimenta este comportamiento, puede cerrar la ayuda contextual pulsando algunas veces en el gráfico.

- Los datos se renuevan automáticamente cada minuto en la consola. Esta actividad es esencial y no se puede poner en pausa, detener u ocultar.
- Si no hay datos disponibles para un cuadro de resumen de estado o gráfico, se visualiza un mensaje informativo.

Sucesos

- El estado de los indicadores que se muestran junto al título de la pestaña **Sucesos**, como **14** **3**, muestran un recuento de las gravedades de suceso más altas para el elemento de navegador seleccionado: aplicación, grupo, subgrupo o instancia. Las gravedades de umbral están consolidadas, tal como se muestra en la tabla siguiente. Por ejemplo, **Sucesos** significa que el suceso de gravedad más alto es leve o de aviso.

Pestaña Sucesos	Gravedad de umbral
Crítico	Muy grave y Crítico
Aviso	Leve y Aviso
Normal	Desconocido

  Cuando el entorno gestionado incluye IBM Operations Analytics - Predictive Insights y se detecta una anomalía, se abre un suceso. Un icono en forma de rombo recubre el indicador de estado, como por ejemplo , para notificarle que Operations Analytics - Predictive Insights ha detectado al menos una anomalía. Por ejemplo, **Sucesos** , indica que el suceso de estado más elevado es Aviso y que hay al menos un suceso de anomalía abierto.
- Pulse la pestaña **Sucesos** para ver un resumen del recuento total de sucesos, un recuento de cada tipo de gravedad y un indicador de porcentaje de las gravedades. Para obtener más información, consulte “Estado de suceso” en la página 1143.

Vistas personalizadas

Las páginas que crea y guarda se asocian a la aplicación seleccionada. Por ejemplo, la aplicación Gestión de inventario de la Demostración guiada de Cloud APM tiene los agentes de supervisión siguientes: Linux OS, MySQL, Node.js, Hadoop y Ruby. Puede crear y guardar una página personalizada en cualquier nivel del navegador desde aplicación a instancia y a continuación abrirla en el mismo nivel en el que se ha creado. Una página que se crea en un nivel determinado sólo puede abrirse en el mismo nivel. Las métricas disponibles para los widgets pueden ser de cualquiera de los recursos de la aplicación. Con el ejemplo de Gestión de inventario, puede crear una página con una tabla del Agente de Ruby, un gráfico del Agente de sistema operativo Linux, etc.

- La pestaña **Vistas personalizadas** está disponible en cualquier nivel del navegador al seleccionar una aplicación desde **Todas mis aplicaciones**.
- Después de abrir la pestaña **Vistas personalizadas**, se muestra la ventana **Seleccione una plantilla para la página personalizada** o la página predeterminada si esta ya se ha establecido.
  - En la ventana **Seleccionar una plantilla para la página personalizada**, puede seleccionar una plantilla para crear una página.
  - En la página predeterminada, puede pulsar para crear una página nueva.
- En la página predeterminada, pulse en la lista de páginas y seleccione una de las páginas guardadas de la lista.
- Las opciones que ve en la pestaña Vistas personalizadas varían en función de si una página se está editado o visualizado. Para obtener información sobre la edición de una página, consulte “Creación y

gestión de páginas personalizadas” en la página 1147. Para obtener información sobre la visualización de una página, consulte “Visualización de páginas personalizadas” en la página 1154.

Manipulación del widget Topología de transacciones agregada

Utilice el widget **Topología de transacciones agregada** para ver la jerarquía de recursos en la aplicación seleccionada. Puede ajustar y moverse por la pantalla para ver el estado de cada componente y su relación con otros componentes, y abrir el panel de instrumentos correspondiente a un nodo.

Antes de empezar

Después de seleccionar una aplicación en el Panel de instrumentos del rendimiento de aplicaciones, la pestaña **Visión general de estado** aparece con dos o más gráficos, en función de los recursos supervisados que están incluidos en la aplicación.

La **Topología de transacciones agregada** se visualiza para los agentes siguientes que admiten el rastreo de transacciones:

- Agente de DataPower
- Agente de HTTP Server
- Agente de IBM Integration Bus
- Recopilador de datos de J2SE
- Agente de JBoss
- Recopilador de datos de Liberty
- Agente de Microsoft .NET
- Agente de Microsoft SQL Server
- Recopilador de datos de Node.js
- Agente de Supervisión de tiempo de respuesta
- Agente de SAP NetWeaver Java Stack
- Agente de Tomcat
- Agente de WebLogic (solo Linux y Windows)
- Agente de WebSphere Applications
- Agente de WebSphere MQ

La **Topología de transacciones agregada** muestra un objeto de nodo para cada recurso supervisado que soporta la característica de topología.

Procedimiento

Siga uno de estos pasos para manipular el widget **Topología de transacciones agregada** y abrir los paneles de instrumentos asociados a los nodos:

- Para abrir un panel de instrumentos enlazado, efectúe una doble pulsación en el nodo de topología. También puede pulsar el botón derecho del ratón en un nodo y seleccionar una de las opciones de detalle del panel de instrumentos, **Ir a la página Resumen de transacciones** o **Ir a la página Instancia de componente**, o seleccionar **Propiedades** para ver información sobre el sistema gestionado.
- Para aumentar el tamaño de visualización de la topología, pulse **Acercar**. También puede pulsar **Acciones** > **Acercar** si no hay ningún nodo seleccionado.
- Para reducir el tamaño de visualización de la topología, pulse **Alejar**. También puede pulsar **Acciones** > **Alejar** si no hay ningún nodo seleccionado.
- Para ajustar el tamaño de visualización de la topología para que se ajuste al espacio de widget actual, pulse **Ajustar contenido**. También puede pulsar **Acciones** > **Ajustar contenido** si no hay ningún nodo seleccionado.

- Para filtrar los nodos de topología, seleccione uno de los indicadores en la barra de filtro. Puede activar o desactivar los filtros y seleccionar varios filtros. Los nodos con una propiedad que no coincide con el filtro se atenúan, y los nodos que coinciden con el filtro permanecen visibles.
  - Normal, Aviso, Crítico o Desconocido para filtrar por estado de nodo.
  - Para filtrar por entorno, seleccione **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **Local** (IBM Cloud Application Performance Management, Private) , **Nube privada** (IBM Cloud Private) o **Nube pública** (IBM Cloud).
  - Filtro para añadir un filtro personalizado.
- Para hacer más espacio para el widget de topología, pulse **Contraer sección** en el navegador o los widgets de gráfico circundantes, o arrastre un borde del widget.

Grupo e instancia – Panel de instrumentos del rendimiento de aplicaciones

Utilizar el panel de instrumentos para el grupo de aplicaciones, el subgrupo o la instancia seleccionados para obtener un estado de alto nivel de los sistemas gestionados. Puede acceder a paneles de instrumentos detallados con medidas para la instancia seleccionada y crear gráficos y tablas personalizados.

Después de seleccionar una aplicación en **Todas mis aplicaciones** en el Panel de instrumentos del rendimiento de aplicaciones, se visualizan las pestañas **Visión general de estado** y **Sucesos**.

La sección **Grupos** del navegador lista uno o más de varios grupos posibles, en función de los componentes constituyentes de la aplicación definida.

Para obtener una descripción del navegador y de los elementos del banner, consulte "Navigator" en la página 1114, "Buscar" en la página 1114, "Acciones" en la página 1114 y " Ayuda" en la página 1114.

Visión general de estado

Grupos y subgrupos

- Seleccione un grupo o expanda un grupo y seleccione un subgrupo para ver un widget de grupo de resumen para cada sistema gestionado en la aplicación. Después de seleccionar un subgrupo, los widgets de grupo de resumen en la pestaña **Visión general de estado** son específicos de dicho subgrupo.
- En función de los productos de supervisión instalados, están disponibles los grupos predefinidos siguientes:

  Availability Monitoring
  Este grupo se visualiza para las aplicaciones personalizadas. El comportamiento de navegación de Availability Monitoring es diferente de los grupos **Componentes** y **Transacciones**.

  El complemento y los paneles de instrumentos de Availability Monitoring se describen en "Availability Monitoring" en la página 1081.

  Componentes
  Este grupo se visualiza para todas las aplicaciones, con la excepción del Agente de Supervisión de tiempo de respuesta, el Agente de Synthetic Playback y Availability Monitoring.

  Componentes tiene un subgrupo para cada componente de software supervisado que soporta la aplicación seleccionada.

  Transacciones
  Este grupo incluye los subgrupos **Transacciones de usuario final**y **Transacciones sintéticas** (IBM Website Monitoring on Cloud antes del release de agosto de 2017 release). Para obtener más información, consulte la ayuda para Supervisión de transacciones y el Agente de Synthetic

Playback o sus PDF de consulta en APM Developer Center bajo PDF de métricas de agente/consulta.

- Después de seleccionar **Componentes** o un subgrupo de la sección **Grupos**, la pestaña **Visión general de estado** cambia para mostrar un panel de instrumentos de resumen con un widget de grupo para cada recurso gestionado. El entorno de origen se muestra como **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **Local** (IBM Cloud Application Performance Management, Private) , **Nube privada** (IBM Cloud Private) o **Nube pública** (IBM Cloud).. La sección **Instancias** se redenomina para el título de subgrupo y se llena con los nombres de instancia individuales.

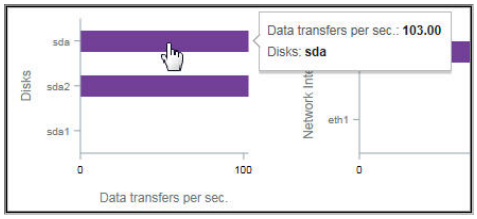
Si la aplicación tiene muchas instancias de sistema gestionado, se visualizan muchos widgets de grupo. Puede desplazarse por la lista para verlos todos. También puede seleccionar un tipo de sistema gestionado en la lista de subgrupos de componentes, como el sistema operativo Windows, para limitar la visualización a los mismos tipos de sistemas gestionados. También puede filtrar las instancias de sistema gestionado.

Sólo para el navegador Firefox: Según el número de agentes y el ancho de banda, a medida que se desplaza hacia abajo en la página Componentes, es posible que vea un mensaje emergente que informa que el script para cargar la página de recursos tardará en completarse. Seleccione la opción, "No volver a preguntar" para inhabilitar el mensaje y continuar abriendo los widgets. De forma alternativa, puede especificar `about:config` en el recuadro de dirección, buscar **`dom.max_script_run_time`** y aumentar el valor de tiempo de espera (en segundos). El valor 0 (cero) inhabilita el tiempo de espera.

Instancias

- Pulse dentro de un widget de grupo o seleccione el nombre de instancia en el navegador para abrir un panel de instrumentos de detalles para el recurso gestionado.
- Si se visualizan muchas instancias en el navegador, utilice el campo de búsqueda en la barra de herramientas Instancias. A medida que escribe, todas las instancias que no coincidan se eliminarán de la visualización.
- Para pausar la renovación automática de Panel de instrumentos del rendimiento de aplicaciones, pulse **Pausar** en la barra de herramientas Instancias; para reanudar la renovación automática, pulse **Reanudar**.
- Los widgets e ICR que se muestran para los sistemas gestionados podrían depender de la versión del agente. Si un agente instalado en el sistema gestionado se encuentra en una versión anterior, es posible que no pueda suministrar tanta información como la versión actual del agente. Se muestra un mensaje en lugar de los ICR en un gráfico o tabla cuando no hay datos disponibles. El motivo podría ser tan simple como que no se hayan notificado datos durante el lapso de tiempo. O bien puede ser debido a que un agente de una versión anterior no es compatible con el conjunto de datos o un atributo incluido en el gráfico o tabla.
  Para ver una lista de los paneles de instrumentos del agente que se han actualizado desde el último reinicio de Servidor de Cloud APM, seleccione **Acciones** > **Registro de panel de instrumentos**.

- Algunos de los widgets del panel de instrumentos muestran métricas que se basan en un rango de tiempo, y otros widgets muestran las métricas más recientes. Si se muestra una barra de selección de tiempo, puede ajustar el periodo de tiempo del panel de instrumentos que afecta a los gráficos o a las tablas cuyos valores se derivan de las muestras de datos históricas. Para obtener más información, consulte "Ajuste y comparación de métricas a lo largo del tiempo" en la página 1125. Mientras visualiza gráficos, puede pulsar un punto de gráfico para abrir una ayuda contextual con el valor del punto de gráfico y demás información pertinente. Después de visualizar un gráfico de líneas en el navegador Internet Explorer Versión 11, quizá siga viendo la ayuda contextual mientras mueve el cursor alrededor de la ventana. Si experimenta este comportamiento, puede cerrar la ayuda contextual pulsando algunas veces en el gráfico.
- Si observa un gráfico al que le faltan barras, significa que el valor es 0 (cero) para ese punto de datos.



- Los usuarios de IBM Cloud Application Performance Management, Advanced tienen paneles de instrumentos de diagnósticos adicionales a los que se accede pulsando el enlace **Diagnosticar** desde un widget de grupo en el panel de instrumentos de detalles.

  Restricción: El sistema gestionado para el que está abriendo los paneles de instrumentos de diagnóstico debe residir en el dominio de IBM Cloud APM. Si el sistema gestionado reside en el dominio de origen de IBM Cloud o IBM Tivoli Monitoring, los paneles de instrumentos de diagnóstico no están disponibles. Vea también "Coexistencia del agente de Cloud APM y el agente de Tivoli Monitoring" en la página 984.
- Si el entorno incluye el Agente de Synthetic Playback, puede ejecutar informes de Cloud APM para la instancia de agente desde el menú **Acciones**.

Sucesos

- El estado de los indicadores que se muestran junto al título de la pestaña **Sucesos**, como **14** **3**, muestran un recuento de las gravedades de suceso más altas para el elemento de navegador seleccionado: aplicación, grupo, subgrupo o instancia. Las gravedades de umbral están consolidadas, tal como se muestra en la tabla siguiente. Por ejemplo, **Sucesos** significa que el suceso de gravedad más alto es leve o de aviso.

Pestaña Sucesos	Gravedad de umbral
Crítico	Muy grave y Crítico
Aviso	Leve y Aviso
Normal	Desconocido

  Cuando el entorno gestionado incluye IBM Operations Analytics - Predictive Insights y se detecta una anomalía, se abre un suceso. Un icono en forma de rombo recubre el indicador de estado, como por ejemplo , para notificarle que Operations Analytics - Predictive Insights ha detectado al menos una anomalía. Por ejemplo, **Sucesos** , indica que el suceso de estado más elevado es Aviso y que hay al menos un suceso de anomalía abierto.
- Pulse la pestaña **Sucesos** para ver un resumen del recuento total de sucesos, un recuento de cada tipo de gravedad y un indicador de porcentaje de las gravedades. Para obtener más información, consulte "Estado de suceso" en la página 1143.

Vistas personalizadas

Las páginas que crea y guarda se asocian a la aplicación seleccionada. Por ejemplo, la aplicación Gestión de inventario de la Demostración guiada de Cloud APM tiene los agentes de supervisión siguientes: Linux OS, MySQL, Node.js, Hadoop y Ruby. Puede crear y guardar una página personalizada en cualquier nivel del navegador desde aplicación a instancia y a continuación abrirla en el mismo nivel en el que se ha creado. Una página que se crea en un nivel determinado sólo puede abrirse en el mismo nivel. Las métricas disponibles para los widgets pueden ser de cualquiera de los recursos de la aplicación. Con el ejemplo de Gestión de inventario, puede crear una página con una tabla del Agente de Ruby, un gráfico del Agente de sistema operativo Linux, etc.

- La pestaña **Vistas personalizadas** está disponible en cualquier nivel del navegador al seleccionar una aplicación desde **Todas mis aplicaciones**.
- Después de abrir la pestaña **Vistas personalizadas**, se muestra la ventana **Seleccione una plantilla para la página personalizada** o la página predeterminada si esta ya se ha establecido.
  - En la ventana **Seleccionar una plantilla para la página personalizada**, puede seleccionar una plantilla para crear una página.
  - En la página predeterminada, puede pulsar  para crear una página nueva.
- En la página predeterminada, pulse en la lista de páginas y seleccione una de las páginas guardadas de la lista.
- Las opciones que ve en la pestaña Vistas personalizadas varían en función de si una página se está editado o visualizado. Para obtener información sobre la edición de una página, consulte “Creación y gestión de páginas personalizadas” en la página 1147. Para obtener información sobre la visualización de una página, consulte “Visualización de páginas personalizadas” en la página 1154.

Detalles de atributo

- La pestaña **Detalles de atributo** se visualiza después de seleccionar una instancia de componente desde la sección **Instancias** del navegador (se ha cambiado el nombre por el nombre del subgrupo seleccionado) o pulsando dentro de un widget de grupo de resumen.
- Si las páginas de gráfico o de tabla se han guardado para el agente, la página abierta más recientemente se visualiza con las métricas de la instancia de componente seleccionada. Pulse en el título ⌄ para seleccionar otra página guardada desde **Mis páginas** › o **Páginas compartidas** ›.
- Puede editar el gráfico o la tabla y pulsar **Previsualizar resultados** para representar el gráfico o la tabla con los atributos seleccionados. Para otras opciones, consulte “Creación de una página de tablas o un gráfico personalizados” en la página 1127.

Edición de los widgets del grupo del panel de instrumentos Componentes

Puede editar los valores de umbral de los widgets de grupo que se visualizan en el panel de instrumentos **Componentes** (seleccionado en la sección **Grupos** del navegador). También puede controlar qué widgets de grupo se visualizan y su posición, y decidir si un umbral de widget se debe incluir en la determinación del estado del componente.

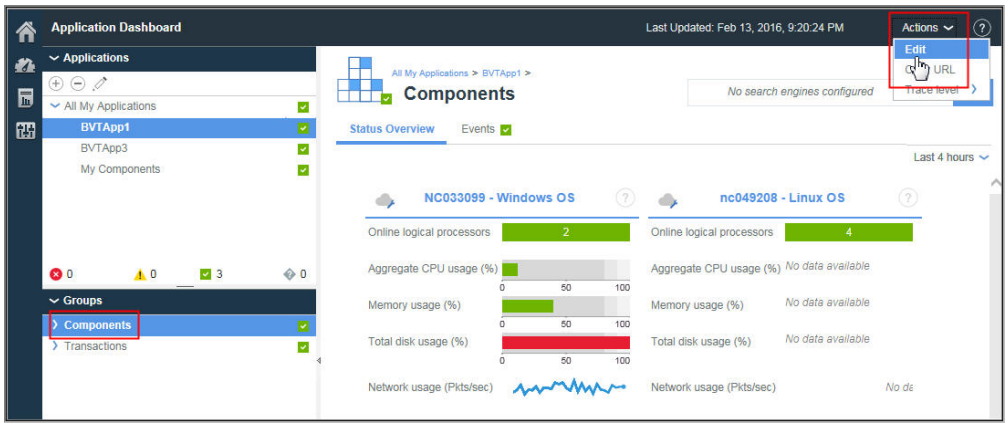
Acerca de esta tarea

Esta tarea implica editar el panel de instrumentos de grupo Componentes y su widget de grupo de resumen constituyente para una aplicación definida. El editor del grupo Componentes no está disponible para la aplicación predefinida **Mis componentes**. Para más información sobre aplicaciones definidas, consulte “Gestión de aplicaciones” en la página 1133.

El ID de usuario también debe tener el permiso de modificación para Panel de instrumentos del rendimiento de aplicaciones y el permiso de creación para Aplicaciones. Para obtener más información, consulte “Roles y permisos” en la página 1036.

Procedimiento

1. Después de abrir el Panel de instrumentos del rendimiento de aplicaciones desde el menú **Rendimiento**, seleccione la aplicación cuyos widgets de grupo de resumen de desea editar desde el panel de instrumentos **Todas mis aplicaciones**.
2. En la sección **Grupos** del navegador, pulse **Componentes** para abrir un panel de instrumentos que muestra los widget de grupo de todos los componentes en la aplicación.
3. Pulse **Acciones** > **Editar** para abrir el editor de los widgets de grupo en el grupo **Componentes**.
   Solo se muestra la opción **Editar** cuando el panel de instrumentos **Componentes** está abierto.



4. Realice cualquiera de los cambios siguientes a los widgets de grupo:
   - Para eliminar un widget de grupo de la vista, pulse .
   - Para modificar los umbrales de resumen de un widget, pulse **Valores**, seleccione la pestaña **Umbrales** y cambie los valores de umbral para las gravedades crítico, de aviso o normal. Después de editar los umbrales para el widget de grupo, pulse **Terminado**.
   - Para añadir un widget, pulse , pulse iconos de aplicaciones hasta que se visualice el que desea, pulse dentro del widget de grupo para seleccionarlo, y pulse **Añadir**.
   - Para cambiar el tamaño de un widget, arrastre el icono de tirador . Cambiar el tamaño de un widget no cambia el tamaño del texto ni la altura del widget.
   - Para mover un widget, arrástrelo a una nueva posición.
5. Para guardar los cambios y cerrar el editor, pulse **Guardar**; o para descartar los cambios, pulse **Cancelar**.

Resultados

Se visualiza el panel de instrumentos **Componentes** de la aplicación seleccionada con la nueva configuración.

Qué hacer a continuación

Para obtener más información sobre el panel de instrumentos cuando se selecciona un grupo o subgrupo en el navegador, consulte "Grupo e instancia – Panel de instrumentos del rendimiento de aplicaciones" en la página 1121; para obtener más información sobre el panel de instrumentos del componente supervisado, pulse el botón en el banner **Panel de instrumentos de aplicaciones**.

Ajuste y comparación de métricas a lo largo del tiempo

Algunos de los gráficos del panel de instrumentos muestran métricas que se basan en un periodo de tiempo, y otros gráficos muestran solo las métricas más recientes. Cuando se visualiza un selector de tiempo en la pestaña **Visión general de estado** de una instancia de sistema gestionado, puede ajustar el intervalo de tiempo para los gráficos cuyos valores se derivan de muestras de datos históricos. Para atributos que tienen datos recopilados para para varios días presentados en un gráfico de líneas, puede comparar los valores de hoy con los de un día anterior.

Antes de empezar

Si está realizando la comparación con un intervalo de tiempo de un día anterior, el tiempo que puede retroceder depende del número de días que el Servidor de Cloud APM haya guardado y el tipo de datos visualizados en la página. . Para los suscriptores de pago de Cloud APM, los ejemplos de datos se almacenan durante 8 días para la mayoría de los conjuntos de datos de supervisión de recursos. El número exacto se publica en la ayuda de atributos del agente o recopilador de datos y en el PDF de consulta. (consulte Capítulo 2, “Documentación en PDF”, en la página 43). Para los suscriptores de prueba de Cloud APM, los ejemplos de datos de supervisión de recursos se almacenan durante 2 días. Los datos de rastreo de transacciones de Agente de Supervisión de tiempo de respuesta o los agentes de middleware solo pueden visualizarse de las últimas 24 horas (o de las últimas 4 horas en algunos casos) y su periodo de retención no puede cambiarse.

Procedimiento

Siga estos pasos para ajustar el intervalo de tiempo que se visualiza en el diagrama de líneas para una instancia de recurso gestionado o comparar los valores con el mismo intervalo de tiempo de un día anterior.

1. Si no se muestra el Panel de instrumentos del rendimiento de aplicaciones, selecciónelo en el menú **Rendimiento**.
2. Vaya a la página del panel de instrumentos correspondiente a una instancia que muestre gráficos de línea históricos y pulse el selector de tiempo **Últimas 4 horas**.
3. Seleccione una o más de las opciones siguientes:
   - Para cambiar el intervalo de tiempo mostrado, seleccione **Últimas 4 horas**, **Últimas 12 horas** o **Último día**.
   - Para comparar el intervalo de tiempo visualizado en un gráfico de líneas con las métricas de otro día, seleccione **Comparar con** y seleccione un día anterior hasta el número de días mostrado en el calendario emergente como disponibles (se traza una línea a lo largo de las fechas no disponibles).
   - Para que el intervalo de tiempo se aplique a los paneles de instrumentos de todas las aplicaciones definidas en su entorno supervisado, seleccione **Todas las aplicaciones**. De lo contrario, deje el valor en **Solo esta aplicación** para aplicar el intervalo de tiempo únicamente a la aplicación actual (como "Mis componentes"). La selección **Comparar con** sólo es efectiva en la página actual.

Resultados

- Si va a visualizar datos históricos sin comparación, todos los paneles de instrumentos de la aplicación (o aplicaciones) actual se ven afectados por el cambio.
- Si está viendo una comparación, sólo se ven afectados los gráficos de líneas de la página actual. Se traza una línea para cada ICR para mostrar las métricas del día elegido. Algunos gráficos de líneas no están disponibles para comparación, tal como lo indica la marca de agua del gráfico: "No disponible para comparación". Esto puede ocurrir con recursos recién gestionados que todavía no hayan recopilado datos para la fecha especificada. Intente seleccionar una fecha más reciente para la comparación.
- Los widgets para los cuales no se recopilan datos históricos siguen mostrando los valores más recientes.
- Los puntos de datos se distribuyen a lo largo de toda la longitud del diagrama para el intervalo de tiempo seleccionado. Las indicaciones de fecha y hora se visualizan en la etiqueta del eje, empezando con la indicación de fecha y hora más temprana y finalizando con la más reciente. Compruebe la muestra de datos de mayor antigüedad para confirmar si se visualiza un rango parcial o el rango completo de datos históricos.
- Los datos enviados a los gráficos y las tablas se normalizan a GMT (hora media de Greenwich). El eje **Indicación de fecha y hora** imprime las indicaciones de fecha y hora en el huso horario de su navegador. Si su zona horaria utiliza la hora estándar y el horario de verano, la indicación de fecha y hora mostrada durante la hora de transición se desplaza una hora. Tenga en cuenta, por ejemplo, que está visualizando un gráfico de líneas en España y que la hora cambia de las 2:00 AM (horario estándar)

a las 3:00 AM (horario de verano). La discrepancia entre la GMT de los datos y la hora local de la indicación de fecha y hora provoca que las indicaciones de fecha y hora tengan un hueco de una hora entre las 2:00 AM y las 3:00 AM. Si visualiza el mismo gráfico en Nueva Zelanda durante el cambio de las 3:00 AM (horario de verano) a las 2:00 AM (horario estándar), las indicaciones de fecha y hora entre las 2:00 AM y las 3:00 AM se repiten.

Visualización y gestión de gráficos y tablas personalizados

El Panel de instrumentos del rendimiento de aplicaciones proporciona paneles de instrumentos predefinidos de los indicadores clave de rendimiento del sistema gestionado. Mientras visualiza el panel de instrumentos de la instancia de un componente, utilice la pestaña **Detalles de atributo** para ver páginas de gráficos o tablas guardadas y para crear y gestionar otras páginas.

Por ejemplo, puede ver un indicador crítico en el panel de instrumentos de resumen e ir hasta la instancia donde se ha producido la condición. Desde aquí, puede añadir un gráfico que represente la proporción de CPU ocupada para ver lo que ocurre a lo largo del tiempo. Puede ver detalles sobre los atributos disponibles de la instancia de componente seleccionada y guardar el gráfico o la tabla personalizados con el agente para visualizarlos siempre que abra una instancia de sistema gestionado.

Un subconjunto de los atributos y conjuntos de datos del agente está disponible para su uso en gráficos y tablas personalizados. Estos atributos son los más útiles para visualizar en paneles de instrumentos. El conjunto completo de atributos está disponible para su uso en umbrales personalizados (consulte “Gestor de umbrales” en la página 1019).

Para mejorar el rendimiento y reducir la redundancia, los agentes restringen el número de filas que se muestran para ciertos conjuntos de datos en los Detalles de atributo. Las descripciones de conjunto de datos de la ayuda del agente y el PDF de referencia indican si la muestra de datos predeterminada limita el número de filas que se envían al Servidor de Cloud APM.

Para los usuarios con discapacidad visual, la posibilidad de crear tablas históricas proporciona una alternativa a los diagramas de líneas, que las tecnologías de asistencia, como el software lector de pantalla no puede interpretar. Por este motivo, la pestaña **Detalles de atributo** está disponible para las instancias de transacciones del Agente de Supervisión de tiempo de respuesta y del Agente de Synthetic Playback para crear tablas históricas. Para obtener más información, consulte “Ejemplo de creación de una tabla personalizada con controles de teclado” en la página 1130.

Creación de una página de tablas o un gráfico personalizados

Mientras visualiza Panel de instrumentos del rendimiento de aplicaciones para una instancia de componente, puede seleccionar la pestaña **Detalles de atributo** para ver páginas de tablas o gráficos guardados y para crear y gestionar otras páginas.

Acerca de esta tarea

Después de descender a mayor nivel de detalle desde la página de inicio de Panel de instrumentos del rendimiento de aplicaciones a una instancia del recurso gestionado, la pestaña **Detalles de atributo** se añaden a las pestañas **Visión general de estado** y **Sucesos** en la página del panel de instrumentos.

Estas instrucciones son para crear tablas y gráficos personalizados para instancias de componentes. Puede seguir los pasos para las instancias de transacciones de Agente de Supervisión de tiempo de respuesta y Agente de Synthetic Playback, con las siguientes limitaciones: solamente tablas históricas (sin gráficos); no puede filtrar la lista **Conjunto de datos** o **Atributos**; todos los atributos están seleccionados (no puede seleccionar o deseleccionar atributos individuales); no puede guardar la página: y la opción **Anterior** del selector de tiempo no está disponible para Agente de Synthetic Playback.

Procedimiento

Complete los pasos siguientes para construir un gráfico o una tabla a partir de cualquiera de los conjuntos de datos que están disponibles para la instancia de componente seleccionada:

1. Después de abrir el Panel de instrumentos del rendimiento de aplicaciones desde el menú **Rendimiento**, descienda a mayor nivel de detalle hasta una instancia del recurso gestionado.

El sistema seleccionado se resalta en la sección **Instancias** del navegador, que se denomina según el tipo de componente, como por ejemplo **Ruby App**.

2. Pulse la pestaña **Detalles de atributo**.

   Si no se ha guardado ninguna página de gráficos o de tablas para este tipo de agente de supervisión, se selecciona la **Tabla Tiempo real**. Tiempo real es adecuada para los conjuntos de datos que devuelven varias filas y solo está disponible para tablas.

3. Si se visualiza una página de tablas o gráficos guardada, pulse **Nuevo**.
4. Especifique un nombre para la página de tablas o gráficos en el campo de título.

   No utilice ninguno de los caracteres siguientes en el título: ! " % & ' * ? < > } { \.

5. Si prefiere ver ejemplos de datos a lo largo del tiempo, cambie el tipo a **Histórico**.

   La opción **Gráfico** está habilitada.

6. Si ha seleccionado **Histórico** y prefiere una representación gráfica en lugar de una tabla, pulse **Gráfico**.
7. En la lista **Conjunto de datos**, seleccione el botón del tipo de atributo que desea ver. Si la lista es larga, utilice el recuadro de filtro para reducir la lista especificando el texto que debe incluirse en el nombre del conjunto de datos.
   Por ejemplo, "config" para los filtros del sistema operativo Linux, filtra los conjuntos de datos para mostrar únicamente los conjuntos de datos **Linux_CPU_Config** y **Linux_OS_Config**.
8. Para incluir un atributo en el gráfico o la tabla, marque el recuadro de selección situado junto al nombre en la lista **Atributos**; para incluir todos los atributos, marque el recuadro al principio de la lista. Escriba texto en el recuadro de filtro para localizar atributos específicos, como "porcentaje".
   Por ejemplo, "porcentaje" en el conjunto de datos KLZ_VM_Stats filtra la lista para mostrar **Almacenamiento virtual libre (Porcentaje)** y 5 atributos "Porcentaje" más.

   Los gráficos solo pueden trazar valores numéricos; cualesquiera atributos de tiempo o texto están inhabilitados.

9. Pulse **Previsualizar resultados** para generar la página con el conjunto de datos elegido, una columna de tabla o una agrupación de líneas de gráfico para cada atributo, y una fila o un punto de trazo para cada ejemplo de datos.

   También obtiene una fila o una línea trazada para la agregación de todos los valores.

10. Para ocultar las líneas de gráfico o filas de tabla, realice uno de los pasos siguientes:

Opción	Descripción
Gráfico	Oculte una métrica (una línea en el gráfico) quitando la marca al lado del nombre en la leyenda. Marque un recuadro de selección para visualizar una medida.
Tabla	Reduzca el número de filas que se visualizan especificando el valor de filtro en el recuadro de filtro . También puede crear un filtro avanzado, tal como se describe en “Definición de un filtro de tabla” en la página 1131.

11. Para ajustar el intervalo de tiempo, utilice el selector de tiempo:

Opción	Descripción
Tiempo real	Solo para tablas, renueva y muestra solo el muestreo de datos más reciente.
2 horas	Traza un punto o añade una fila para cada muestra de datos que se ha tomado a intervalos en las últimas dos horas.
4 horas	Traza un punto o añade una fila para cada muestra de datos que se ha tomado a intervalos en las últimas cuatro horas.
12 horas	Traza un punto o añade una fila para cada muestra de datos que se ha tomado a intervalos en las últimas 12 horas.
24 horas	Traza un punto o añade una fila para cada muestra de datos que se ha tomado a intervalos en las últimas 24 horas.

Opción	Descripción
Anterior	Submenú de opciones para incluir datos desde el mimo periodo de tiempo **Ayer**, **Hace 2 días**, o desde cualquier día hasta **Hace una semana**. Por ejemplo, son las 14:10 del 22 de agosto y establece el gráfico o la tabla de modo que muestre las últimas 4 horas. Al seleccionar **Anterior** > **Hace una semana**, puede ver puntos de datos desde las 10:10 a las 14:10 de hoy y desde las 10:10 a las 14:10 PM del 15 de agosto. Después de seleccionar un día anterior, el selector de tiempo muestra un asterisco (*) como por ejemplo Last 4 hours* y se vuelve a generar la tabla de datos del día seleccionado:

- Solamente es posible ver datos del día de hoy y hasta una semana atrás (incluso si ha aumentado el período de retención máximo de datos históricos a más de 8 días).
- Los gráficos históricos se trazan desde la muestra de datos más antigua a la más reciente durante el período de tiempo seleccionado, por ejemplo, las últimas 4 horas. Cuando se selecciona un día anterior, verá los datos desde el rango de tiempo seleccionado el día anterior y el rango de tiempo del día de hoy. Los días que se hallen entre la fecha anterior y hoy mostrarán un punto de gráfico con una indicación de fecha y hora y sin muestras de datos.
- Las tablas históricas se trazan en orden cronológico en orden cronológico descendente. Cuando un día anterior se selecciona para Agente de Supervisión de tiempo de respuesta, cada columna se duplica para el día anterior con "Anterior" en la cabecera de columna.
- Independientemente del intervalo de tiempo seleccionado, puede visualizarse un máximo de 11.000 filas. Por ejemplo, si elige mostrar 12 horas de un conjunto de datos que envía 7.000 filas en 2 horas, se devolverán menos de 3 horas de datos históricos y se visualizarán las muestras de datos más antiguas.

12. Para guardar o hacer otros cambios en el gráfico o la tabla, seleccione una de las opciones siguientes:

Opción	Descripción
Editar	Le devuelve al editor para realizar cualquiera de los cambios siguientes: • Editar el título • Cambiar a muestras de datos en **Tiempo real** o **Históricas** • Ir a **Gráfico** o **Tabla** • Seleccionar un **Conjunto de datos** o **Atributos** distintos
Nuevo	Descarga todos los cambios no guardados en la vista actual y le devuelve a la página de selección para crear un nuevo gráfico o una nueva tabla.
Cancelar	Cancela la sesión de edición para la página actual de gráfico o tabla.
Suprimir	Suprime la página. **Suprimir** está disponible sólo después de guardar una página y cancelar cualquier edición actual.
Guardar para mí	Guarda la página de gráfico o de tabla para que la vea solo su ID de usuario. Ningún otro usuario puede ver la página guardada.
Guardar para compartir	Guarda la página de gráfico o de tabla para que la vea cualquier ID de usuario que inicie sesión en la Consola de Cloud APM

Las vistas que usted haya guardado tienen un icono de cerradura abierta junto al título. Las vistas que otro usuario haya guardado y que usted no tenga autorización para editar tienen un icono de cerradura cerrada.

Resultados
Después de guardar el gráfico o la tabla personalizados, estos se añaden a la lista de páginas guardadas. La próxima vez que seleccione una instancia del mismo tipo de origen de datos, como WebSphere Applications, y seleccione la pestaña **Detalles de atributo**, se visualiza la página guardada abierta más recientemente. Pulse en el título ⌄ para seleccionar otra página guardada desde **Mis páginas** › o **Páginas compartidas** ›.

Qué hacer a continuación
Repita este procedimiento para crear y gestionar otras páginas de tabla o gráfico.

Para obtener ayuda para crear una tabla utilizando los controles del teclado en lugar de pulsaciones con el ratón, consulte "Ejemplo de creación de una tabla personalizada con controles de teclado" en la página 1130.

Ejemplo de creación de una tabla personalizada con controles de teclado
Los usuarios con discapacidades visuales pueden utilizar la pestaña de panel de instrumentos **Detalles de atributo** para crear tablas históricas como una alternativa accesible a gráficos de líneas históricos que las tecnologías de asistencia como por ejemplo el software lector de pantallas, no pueden interpretar.

Acerca de esta tarea
El ejemplo siguiente ilustra el uso de controles de teclado para crear una tabla histórica para transacciones notificadas por el Agente de Synthetic Playback. Para obtener más información sobre el agente, consulte "Gestión de transacciones sintéticas y sucesos con Website Monitoring" en la página 1061.

Al pulsar la tecla Tabulador, el foco pasa al siguiente campo o a la siguiente sección de la ventana de aplicación, de izquierda a derecha y de arriba abajo. Puede utilizar estos pasos para generar una tabla de transacciones para el Agente de Supervisión de tiempo de respuesta sustituyendo **Mis transacciones** con una aplicación que incluya el agente o para generar una tabla para una instancia de componente sustituyendo **Mis transacciones** por otra aplicación y seleccionando el grupo **Componentes**.

Procedimiento

Siga estos pasos para crear una tabla de transacciones para crear una tabla de transacciones del Agente de Synthetic Playback en la pestaña **Detalles de atributo** mediante los atajos de teclado:

1. Inicie la sesión en IBM Cloud Application Performance Management.

   El foco está en la barra de navegación.
2. Para abrir Panel de instrumentos del rendimiento de aplicaciones, pulse la flecha abajo para pasar el foco al menú **Rendimiento**, pulse Intro para seleccionarlo, pulse la flecha abajo para la opción de **Panel de instrumentos del rendimiento de aplicaciones** y vuelva a pulsar Intro.
3. Para abrir la página del panel de instrumentos de **Transacciones sintéticas** pulse el tabulador varias veces (alrededor de 7 veces) hasta que el foco pase al navegador, pulse la flecha abajo para poner el foco en la aplicación predefinida **Mis transacciones** y pulse Intro.
4. Para abrir la página del panel de instrumentos **Detalles de transacciones** pulse el tabulador (alrededor de 10 veces) hasta que el foco pase a la sección **Instancias** en una instancia de transacción de **Transacciones sintéticas** y pulse Intro.

   La pestaña **Detalles de atributo** se visualiza en el panel de instrumentos.
5. Para abrir la pestaña **Detalles de atributo**, pulse el tabulador (alrededor de 6 veces) hasta que el foco pase a la pestaña **Visión general de estado** y pulse la flecha derecha hasta que el foco esté en la pestaña **Detalles de atributo**.

   La **Tabla**  **histórica** y todos los atributos del conjunto de datos **Disponibilidad de transacción a lo largo del tiempo** están seleccionados.
6. Para generar la tabla, pulse el tabulador (alrededor de 18 veces) hasta que el foco esté en el botón **Previsualizar resultados** y pulse Intro.

Resultados
Los atributos de **Disponibilidad de transacción a lo largo del tiempo** se visualizan en una tabla con una columna para cada atributo y una fila para cada ejemplo de datos a lo largo de las últimas 4 horas.

Qué hacer a continuación

- Para reducir el número de filas que se visualizan, puede pulsar el tabulador para poner el foco en el recuadro de texto **Filtro** y especificar un texto completo o parcial o un valor de indicación de fecha y hora por el que filtrar.
- Para cambiar el periodo de tiempo, pase el foco al menú desplegable **Últimas 4 horas** y seleccione otra opción. Para obtener más información consulte el paso "11" en la página 1128 in "Creación de una página de tablas o un gráfico personalizados" en la página 1127.
- Para generar una tabla con el conjunto de datos **Tiempo de respuesta de transacción** pulse el tabulador (alrededor de 2 veces) para pasar el foco a la herramienta **Nuevo** y pulse Intro. Se abre el panel de selección. Seleccione el conjunto de datos **Tiempo de respuesta de transacción** y el botón **Previsualizar resultados**.

Definición de un filtro de tabla
Puede limitar las filas de una tabla que está viendo en la pestaña **Detalles de atributo** del panel de instrumentos para mostrar solo las filas de un tipo determinado o que tengan por valores de atributo de texto o indicación de fecha y hora. Aunque los valores numéricos no están disponibles para el filtrado, como por ejemplo los porcentajes, algunos valores de atributos numéricos se convierten en un valor de visualización para la tabla y se trata como si fuera texto.Puede aplicar un filtro rápido o abrir un editor para componer un filtro avanzado.

Procedimiento

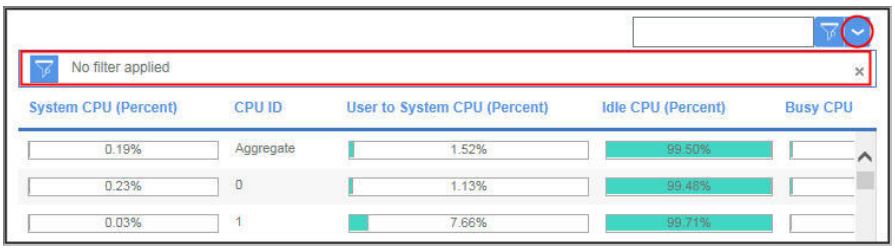
Siga estos pasos para filtrar una tabla personalizada por valores de atributo de texto o indicación de fecha y hora. Aunque los valores numéricos no están disponibles para el filtrado, como por ejemplo los porcentajes, algunos valores de atributos numéricos se convierten en un valor de visualización para la tabla y se trata como si fuera texto.

1. Después de abrir el Panel de instrumentos del rendimiento de aplicaciones desde el menú **Rendimiento**, descienda a mayor nivel de detalle hasta una instancia del recurso gestionado.
2. Pulse la pestaña **Detalles de atributo**.

   Se visualiza la página guardada más recientemente o, si no se ha guardado ninguna página, se visualizan las listas de selección **Conjunto de datos** y **Atributos**.
3. Si se visualiza una página de tabla guardada, siga en el paso "5" en la página 1131, seleccione otra página de tabla guardada en el menú desplegable, o pulse **Añadir** para crear una nueva tabla.
4. Si está creando una nueva tabla o editando una tabla guardada, seleccione el **Conjunto de datos** y los **Atributos** que desea utilizar y pulse **Previsualizar resultados**.
5. Para un filtro rápido, pulse en el cuadro de texto **Filtro** y escriba el texto parcial o completo por el que desea filtrar.

   A medida que escribe, las filas que no contienen lo que ha escrito se eliminan de la tabla. Para eliminar el filtro rápido, suprima el valor o pulse la "x".
6. Para un filtro avanzado, pulse el menú desplegable y seleccione **Crear filtro** o pulse en la barra de filtros.

   Se abre la ventana **Crear filtro** con las reglas que ha definido.



7. Para definir una regla, complete los campos:
   a) Deje el valor de columna en "Cualquier columna" o seleccione el atributo mediante el cual filtrar en la lista.
   b) Deje la condición en "contiene" o seleccione otro operador de la lista y escriba el valor de texto o indicación de fecha y hora por el que filtrar en el recuadro de texto:

Condición	**La fila se incluye en la tabla cuando...**
contiene	el valor de filtro se encuentra en algún lugar de la celda.
igual a	el valor de celda coincide exactamente con el valor de filtro, incluidas las mayúsculas y minúsculas.
empieza por	el valor de celda empieza con los mismos caracteres que el valor de filtro.
termina por	el valor de celda tiene los mismos caracteres al final que el valor de filtro.
no es igual a	el valor de celda no es una coincidencia exacta del valor del filtro.
no contiene	el valor de celda no incluye el mismo texto o número que el valor de filtro.
no empieza por	el valor de celda no empieza con los mismos caracteres que el valor de filtro.
no termina por	el valor de celda no termina con los mismos caracteres que el valor de filtro.
está vacío	la celda no muestra ningún dato.

   c) Después de completar la regla, pulse **Filtrar** para ver los resultados, pulse **Añadir regla de filtro** para añadir otra regla o vaya al paso siguiente.
8. Si el filtro tiene varias reglas, realice cualquiera de estos pasos:
   - **Coincidir** se establece inicialmente en **Todas las reglas**, que significa que una fila sólo se visualiza si los datos de la fila cumplen todas las reglas del filtro. La fila se excluye si ningún valor de texto o indicación de fecha y hora sigue ninguna regla. Si tiene varias reglas y desea que se incluya una fila si cumple cualquiera de las reglas, cambie el valor por **Cualquier regla**.
   - Para editar una regla, cambie cualquiera de los valores de campo.
   - Para suprimir una regla, selecciónela y pulse **Eliminar regla**.
9. Cuando haya terminado de definir una regla (o reglas), pulse **Filtrar** para cerrar el cuadro de diálogo y aplicar el filtro.

Resultados

Los grupos que no cumplen los criterios de filtros se eliminan de la visualización y la barra de filtro informa del número de elementos, por ejemplo, "480 de 1200 elementos mostrados".

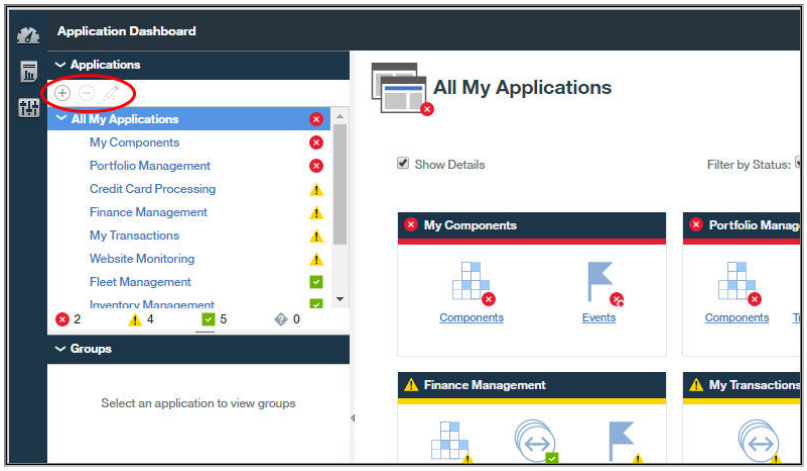
Qué hacer a continuación

- Coloque el puntero del ratón sobre la barra de filtro para abrir una ventana emergente que contiene los criterios de filtro. Puede suprimir una regla (pulsar ×) o pulsar dentro de la ventana para editar los criterios de filtro.
- Pulse **Borrar filtro** en la barra de filtro o **Borrar** en la ventana **Crear filtro** para eliminar el filtro y mostrar todas las filas.

Gestión de aplicaciones

Utilice las herramientas que están disponibles en el Panel de instrumentos del rendimiento de aplicaciones para organizar los recursos gestionados en aplicaciones.

Las herramientas **Aplicaciones** del navegador abren el editor de aplicaciones para crear o editar aplicaciones y aplicar los recursos gestionados disponibles.



La aplicación **Mis componentes** es una aplicación predefinida que incluye los sistemas gestionados que ha descubierto el Servidor de Cloud APM. **Mis Componentes** no se puede editar ni suprimir.

Para obtener una demostración de vídeo sobre cómo añadir una aplicación, vea Application Performance Management - Define Application.

Para obtener un escenario de creación de una aplicación para supervisar la pila de aplicaciones de IBM Java, consulte “Adición de aplicaciones web al Application Performance Dashboard ” en la página 94 y “Asociación de la Pila de aplicaciones Java de IBM con la aplicación web ” en la página 95.

Restricción: Debe tener permiso de modificación para Aplicaciones para utilizar la herramienta Añadir aplicación. Debe tener permiso de modificación para Aplicaciones o la aplicación específica para utilizar las herramientas Eliminar y Editar. Para obtener más información, consulte “Trabajo con roles, usuarios y permisos” en la página 1044.

Adición de una aplicación

Utilice el editor de aplicaciones para crear una nueva aplicación y aplicar los recursos gestionados que no están disponibles o seleccionar una de las aplicaciones descubiertas.

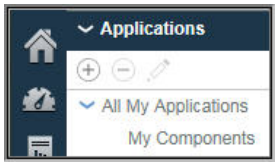
Antes de empezar

Debe tener permiso de modificación para Aplicaciones para utilizar la herramienta Añadir aplicación. Para obtener más información, consulte “Trabajo con roles, usuarios y permisos” en la página 1044.

Procedimiento

Complete los pasos siguientes en Consola de Cloud APM para añadir una aplicación al Panel de instrumentos del rendimiento de aplicaciones.

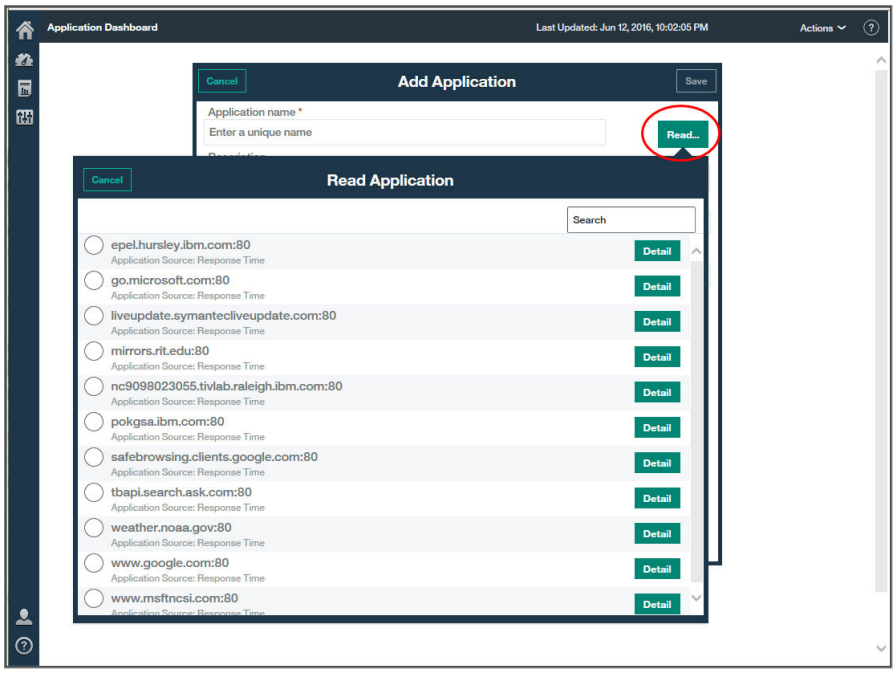
1. Si el Panel de instrumentos del rendimiento de aplicaciones no se visualiza, selecciónelo en el menú **Rendimiento** o, si está en otra página de la consola, pulse el enlace **Inicio**.
2. En la sección **Aplicaciones** del navegador, pulse . Se visualizará la ventana **Añadir aplicación**.



3. Especifique un nombre para la aplicación en el campo **Nombre de la aplicación** y, opcionalmente, una descripción en el campo **Descripción**.

   No utilice los símbolos ! " % & ' * ? < > } { \ en el nombre ni en la descripción.

   Puede ver algunos ejemplos de nombres de aplicación, como por ejemplo "Finance Management" y "Credit Card Processing" en Demostración guiada.
4. Pulse **Leer** para abrir la ventana **Leer aplicación** con una lista de las aplicaciones descubiertas y realice uno o varios de los pasos siguientes:
   - Pulse **Detalle** para ver los componentes de una aplicación.
   - Seleccione la aplicación que desee usar y pulse **Guardar**. La ventana **Leer aplicación** se cierra, el repositorio de origen se muestra en el campo **Aplicaciones leídas desde:** y los componentes se listan en **Componentes de la aplicación**.
   - Pulse **Cancelar** para cerrar la ventana sin escoger una opción.

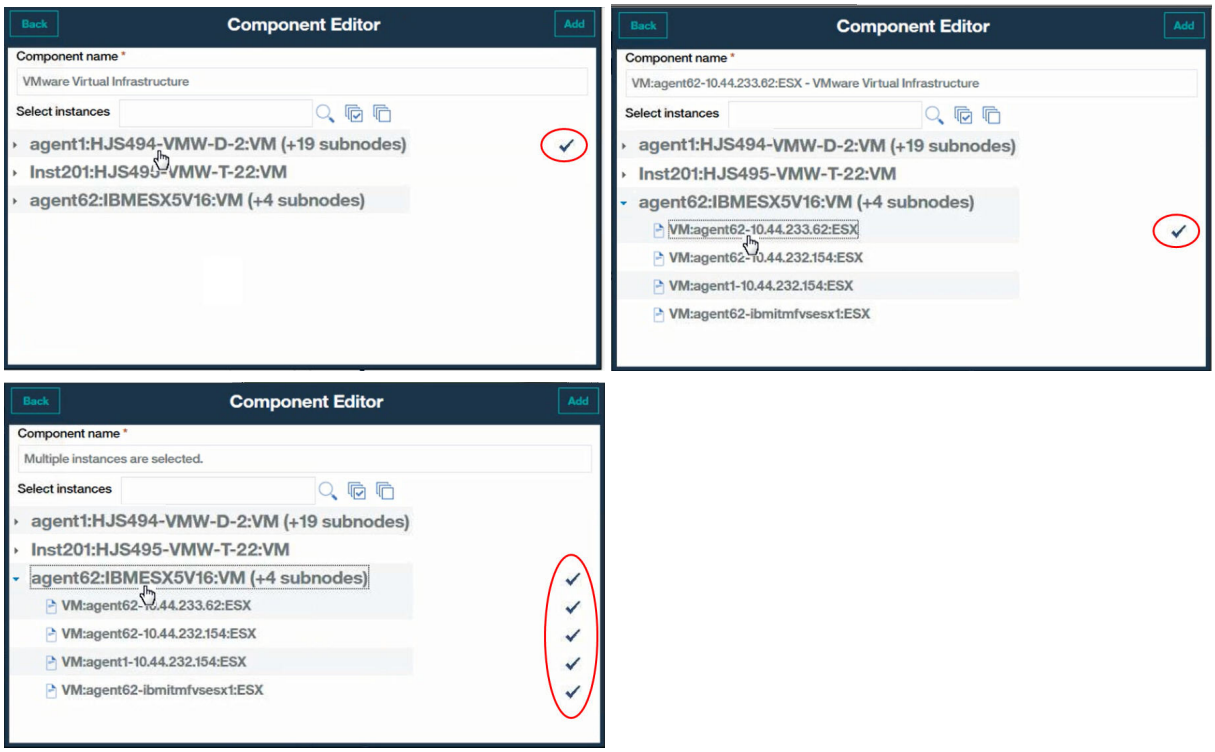


5. En el campo **Plantilla**, conserve la plantilla **Aplicación personalizada** o seleccione una plantilla distinta mediante el botón y pulse en **Guardar**.

   Los tipos de componentes asociados e instancias se mostrarán en la lista **Componentes de la aplicación**.
6. Pulse **Añadir componentes** y, en la ventana **Seleccionar componente** que se abre, seleccione un componente en la lista.

   Se visualizará el **Editor de componentes**.
7. Para buscar y seleccionar instancias de subnodo o nodo de agente (o ambas) para la aplicación, realice uno de los pasos siguientes:
   - Pulse una instancia para seleccionarla.

- Para los nodos de agente que tengan subnodos, seleccione solo el nodo pulsando el nombre mientras el árbol está contraído, seleccione el nodo y todos los subnodos expandiendo el árbol del nodo (pulse ▸) y pulsando el nodo, o bien seleccione subnodos individuales expandiendo el árbol del nodo y pulsando la instancia.
- Utilice la barra de herramientas para buscar instancias que contengan el texto del recuadro de texto de búsqueda, seleccionar todas las instancias o desmarcar todas las instancias.
- Si desea cambiar el nombre de visualización en el navegador, edite el nombre del componente.



V6-V7 Si está añadiendo una instancia de agente de Tivoli Monitoring y no la ve en la lista de instancias disponibles, compruebe que el Tivoli Enterprise Portal Server que está asociado con la Pasarela híbrida tiene una versión soportada (consulte Agentes soportados por la pasarela híbrida (APM Developer Center)).

8. Pulse **Añadir** para añadir los nodos y subnodos de agente seleccionados a la aplicación, pulse **Atrás**.
   La lista Componentes de la aplicación se actualiza con los nombres de componentes nuevos.
9. Seleccione otro componente al que añadir instancias y repita “6” en la página 1134, “7” en la página 1134 y “8” en la página 1135 o pulse **Cerrar**.
10. Si otras instancias están relacionadas con los componentes de la lista **Componentes de la aplicación**, se mostrará un botón que muestra el número de instancias relacionadas y puede realizar los pasos siguientes:
    a) Pulse el botón para ver las instancias relacionadas en la ventana **Detalles actualizados**.
    Se muestra una barra por cada tipo de actualización, incluido el nombre de instancia. Por ejemplo, si se ha eliminado uno de los componentes, aparecerá bajo la barra de componentes **Suprimidos**.
    b) Seleccione una o varias instancias y pulse **Guardar** para actualizar la lista Recursos de la aplicación.
11. Cuando haya acabado de definir la aplicación, cierre el editor de aplicaciones pulsando **Guardar** para guardar los cambios, o pulse **Cancelar** para deshacer los cambios.

Resultados
Las actualizaciones de aplicación las completa el Servidor de Cloud APM después de guardar los cambios. Puede tardar unos minutos antes de que los cambios aparezcan en el panel de instrumentos. (Intente borrar la memoria caché de navegador si los cambios tardan mucho tiempo en visualizarse.) La aplicación

nueva aparece en Panel de instrumentos del rendimiento de aplicaciones y en la sección **Aplicaciones** del navegador. Cuando se selecciona la aplicación, los componentes aparecen en la sección **Grupos**.

Edición de una aplicación

Utilice el editor de aplicaciones para modificar una aplicación definida para añadir o eliminar recursos gestionados como componentes de la aplicación.

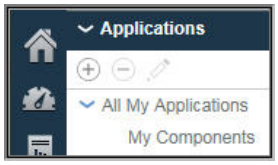
Antes de empezar

Debe tener permiso de modificación para las aplicaciones o la aplicación específica para utilizar la herramienta Editar. Para obtener más información, consulte “Roles y permisos” en la página 1036.

Procedimiento

Siga los pasos siguientes en Consola de Cloud APM para editar una aplicación.

1. Si el Panel de instrumentos del rendimiento de aplicaciones no se visualiza, selecciónelo en el menú **Rendimiento** o, si está en otra página de la consola, pulse el enlace **Inicio**.
2. Seleccione la aplicación que desee editar en la lista **Todas mis aplicaciones** en el navegador y pulse .

   Se visualizará la ventana **Editar aplicación**.
3. Opcional: Edite el **Nombre de la aplicación** o **Descripción**.

   No utilice los símbolos ! " % & ' * ? < > } { \ en el nombre ni en la descripción.
   Si los permisos para ver o modificar aplicaciones son para aplicaciones individuales y no para todas las aplicaciones, es posible que no pueda ver la aplicación en el panel de instrumentos o modificar la aplicación, una vez renombrada. Esta limitación se debe a que la aplicación renombrada se trata como una nueva aplicación. Su rol de administrador o el administrador de la supervisión le debe proporcionar el permiso para ver o modificar para la aplicación renombrada.
4. Si desea añadir componentes e instancias a la aplicación, siga estos pasos.
   a) Pulse y seleccione un componente de la lista en la ventana que se abre.
      Se visualizará el **Editor de componentes**.
   b) Seleccione instancias de subnodo o nodo de agente (o ambas) para la aplicación:
      - Pulse una instancia para seleccionarla.
      - Para nodos que tienen subnodos, seleccione el nodo pulsando el nombre mientras el árbol está contraído, seleccione el nodo y todos los subnodos expandiendo el árbol del nodo (pulse) y pulsando el nodo, o seleccione subnodos individuales expandiendo el árbol del nodo y pulsando la instancia.
      - Utilice la barra de herramientas para buscar instancias que contengan el texto del recuadro de texto de búsqueda, seleccionar todas las instancias o desmarcar todas las instancias.
      - Si desea cambiar el nombre de visualización en el navegador, edite el nombre del componente.
   c) Pulse **Añadir** para añadir la instancia o instancias, y pulse **Atrás**.
      La lista Componentes de la aplicación se actualiza con los nombres de componentes nuevos.
   d) Puede seleccionar otro componente para añadir instancias, o pulsar **Cerrar**.

   La lista Componentes de la aplicación se actualiza con los nombres de componentes nuevos. Un número entre paréntesis después del nombre indica cuántas instancias están asociadas con el componente.

5. Si desea editar un nombre de componente o cambiar la instancia asociada con el mismo, seleccione el componente de la lista **Componentes de la aplicación** y pulse :
   a) Para asociar una instancia distinta con el componente, busque y seleccione la instancia que desee.
   b) Para cambiar el nombre del componente que se utiliza como el nombre de visualización en el navegador para esta aplicación, edite el campo **Nombre de componente**.
   c) Pulse **Guardar**.

   La lista Componentes de la aplicación se actualizará con los cambios que haya realizado.
6. Si desea eliminar un componente o una instancia de la aplicación, selecciónela y pulse . Pulse **Aceptar** para confirmar que desea eliminarla.
7. Si otras instancias están relacionadas con los componentes de la lista **Componentes de la aplicación**, se mostrará un botón que muestra el número de instancias relacionadas y puede realizar los pasos siguientes:
   a) Pulse el botón para ver las instancias relacionadas en la ventana **Detalles actualizados**.
   Se muestra una barra por cada tipo de actualización, incluido el nombre de instancia. Por ejemplo, si se ha eliminado uno de los componentes, aparecerá bajo la barra de componentes **Suprimidos**.
   b) Seleccione una o varias instancias y pulse **Guardar** para actualizar la lista Recursos de la aplicación.
8. Cuando haya acabado de crear o editar la aplicación, cierre el editor de aplicaciones pulsando **Guardar** para guardar los cambios, o **Cancelar** para deshacer los cambios.

Resultados

Las actualizaciones de aplicación las completa el Servidor de Cloud APM después de guardar los cambios. Puede tardar unos minutos antes de que los cambios aparezcan en el panel de instrumentos.

Referencia relacionada

"Roles y permisos" en la página 1036

Supresión de una aplicación

Cuando ya no necesite una aplicación definida para su visualización en el Panel de instrumentos del rendimiento de aplicaciones, puede suprimirla. La supresión de una aplicación no desinstala los componentes de soporte, sólo la aplicación en la que están contenidos. Los mismos componentes están disponibles para añadirlos a otras aplicaciones y no se eliminan de otras aplicaciones a las que pertenezcan.

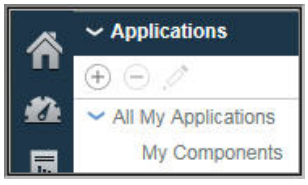
Antes de empezar

Debe tener permiso de modificación para Aplicaciones o la aplicación específica para utilizar la herramienta Eliminar. Para obtener más información, consulte "Trabajo con roles, usuarios y permisos" en la página 1044.

Procedimiento

Complete los pasos siguientes para eliminar una aplicación del Panel de instrumentos del rendimiento de aplicaciones.

1. Si el Panel de instrumentos del rendimiento de aplicaciones no se visualiza, selecciónelo en el menú **Rendimiento** o, si está en otra página de la consola, pulse el enlace **Inicio**.



2. En la sección **Aplicaciones** del navegador, seleccione la aplicación que desee suprimir en la lista **Todas mis aplicaciones** y pulse .

Un mensaje le solicita confirmación.

3. Pulse **Sí** para confirmar que desea suprimir la aplicación; o **No** si no está seguro.

Resultados

Después de pulsar **Sí**, la aplicación se suprimirá del Panel de instrumentos del rendimiento de aplicaciones.

Qué hacer a continuación

Repita este paso para cualquier otra aplicación que desee suprimir.

Visualización y eliminación de agentes fuera de línea

Cuando un agente ha estado fuera de línea durante cuatro días, se elimina de la Consola de Cloud APM. Revise cómo están indicados los agentes fuera de línea y el efecto en grupos de recursos, vistas de topología y otras características. Utilice el editor de aplicaciones para eliminar un sistema gestionado del panel de instrumentos antes de que transcurran cuatro días. .

Acerca de esta tarea

Cuando los agentes se han instalado en los sistemas que se desea gestionar, se conectan al Servidor de Cloud APM y envían muestras de datos al Panel de instrumentos del rendimiento de aplicaciones para la presentación y la evaluación de umbral. Si el agente está fuera de línea, el indicador de estado se muestra en el navegador y en el panel de instrumentos. El servidor espera que pasen un número específico de intervalos sin respuesta del agente antes de mostrar que el agente no está disponible. Consulte "Ejemplos de agentes fuera de línea" en la página 1139.

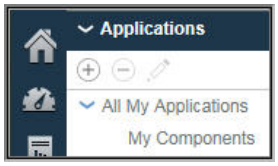
Transcurridos cuatro días, el agente fuera de línea se elimina de la interfaz de usuario con la excepción siguiente: Si el agente es uno que admite el rastreo de transacción, el agente fuera de línea sigue mostrándose en las vistas Topología de transacción de agregado y Topología de instancia de transacción.

Puede eliminar el agente fuera de línea de las aplicaciones definidas, lo que lo elimina de la Consola de Cloud APM antes de que se complete el periodo de espera de cuatro días.

Procedimiento

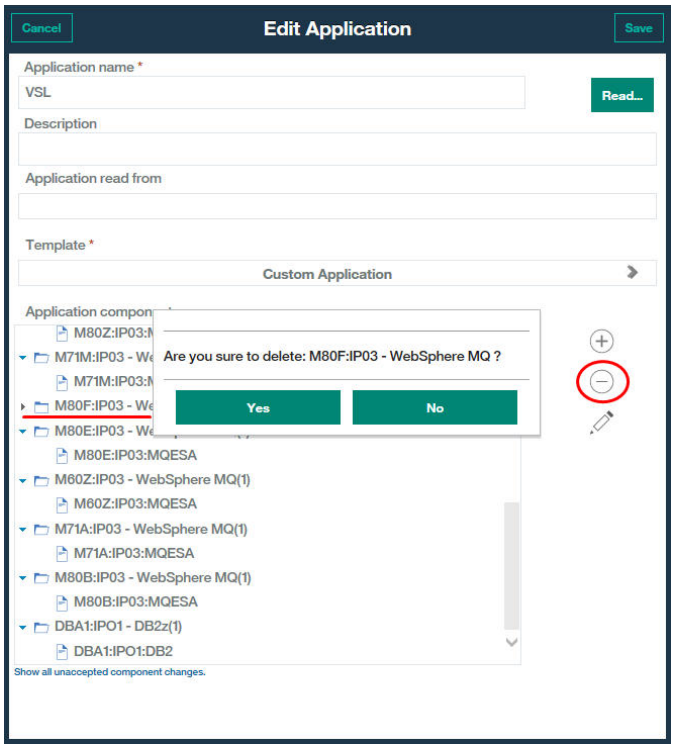
Realice estos pasos para eliminar un agente fuera de línea de una aplicación definida:

1. Si el Panel de instrumentos del rendimiento de aplicaciones no se visualiza, selecciónelo en el menú **Rendimiento** o, si está en otra página de la consola, pulse el enlace **Inicio**.
2. En la sección **Aplicaciones** del navegador, seleccione la aplicación de la que el agente fuera de línea es un componente y pulse **Editar aplicación**.



3. Seleccione el agente o subnodo de agente en la lista Componentes de aplicación y pulse .

   Para los agentes que tengan subnodos, seleccione sólo el agente pulsando el nombre mientras el árbol está contraído, seleccione el nodo y todos los subnodos expandiendo el árbol del nodo (pulse) y pulsando el nodo, o seleccione subnodos individuales expandiendo el árbol del nodo y pulsando la instancia.



4. Cuando haya terminado de editar la aplicación para eliminar el subnodo o agente fuera de línea, pulse **Guardar**.

Resultados

Las actualizaciones de aplicación las completa el Servidor de Cloud APM después de guardar los cambios. Podrían pasar algunos minutos antes de que el agente fuera de línea se elimine del Panel de instrumentos del rendimiento de aplicaciones.

Ejemplos de agentes fuera de línea

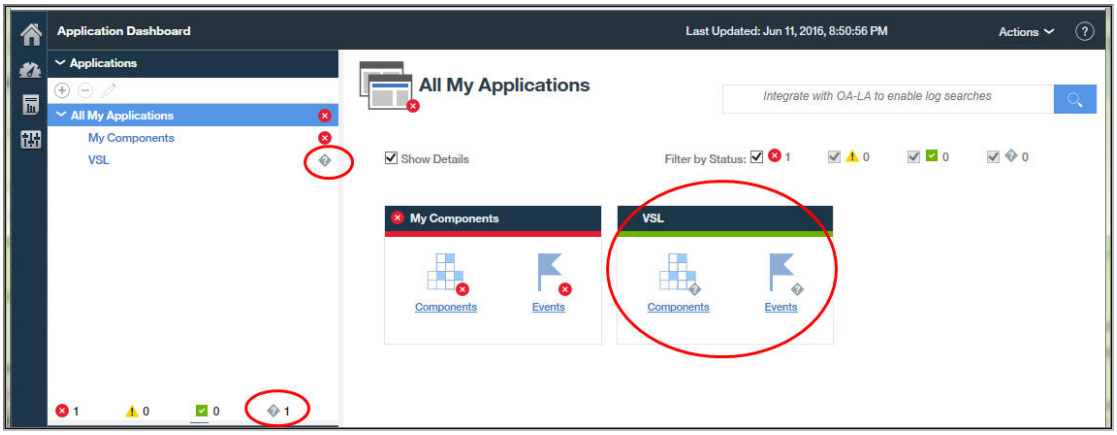
Revise los ejemplos de cómo se visualizan los agentes fuera de línea en la Consola de Cloud APM. Puede eliminar la visualización de cualquier agente fuera de línea que ya no necesite supervisar. Si el agente vuelve a estar en línea posteriormente, la supervisión se reanudará.

Cuando un agente está fuera de línea, no se envían datos a la Consola de Cloud APM y el Panel de instrumentos del rendimiento de aplicaciones visualiza un indicador de estado para el agente y las aplicaciones a las que pertenece. El agente no está disponible para añadirlo a una aplicación definida en el editor de aplicaciones o a un grupo personalizado en el Gestor de grupos de recursos, o para crear tablas o gráficos de líneas históricos en la pestaña Detalles de atributo.

Panel de instrumentos del rendimiento de aplicaciones - Todas mis aplicaciones

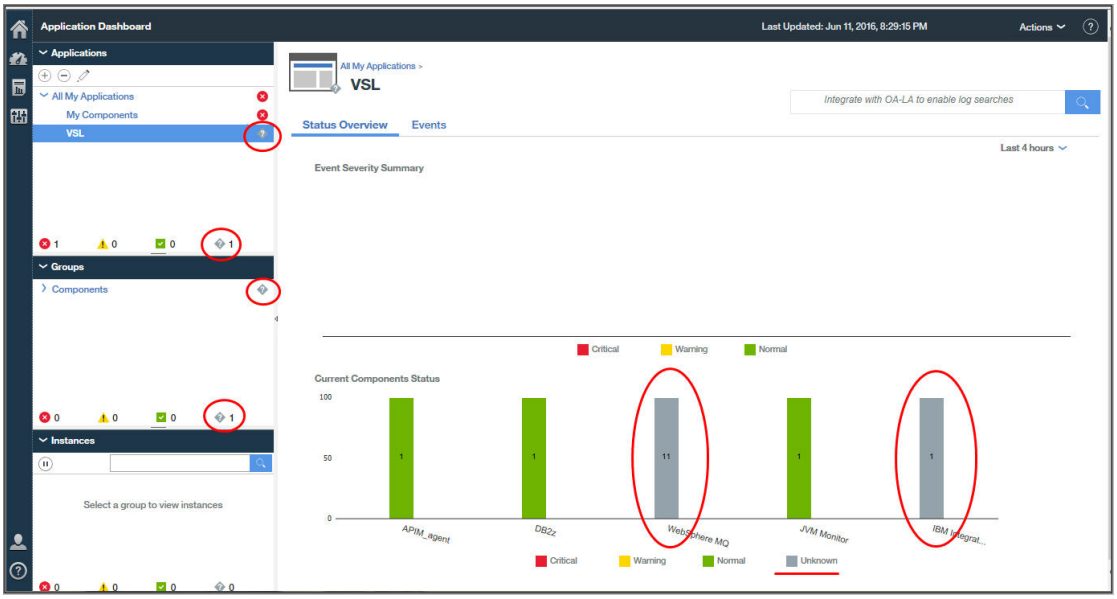
La página de inicio del panel de instrumentos, **Todas mis aplicaciones**, proporciona la primera indicación de estado fuera de línea. El contador de la sección Aplicaciones del navegador muestra el número de aplicaciones con recursos no disponibles.

El recuadro de resumen muestra estado de suceso Normal porque no hay sucesos abiertos para ninguno de los recursos gestionados de la aplicación.



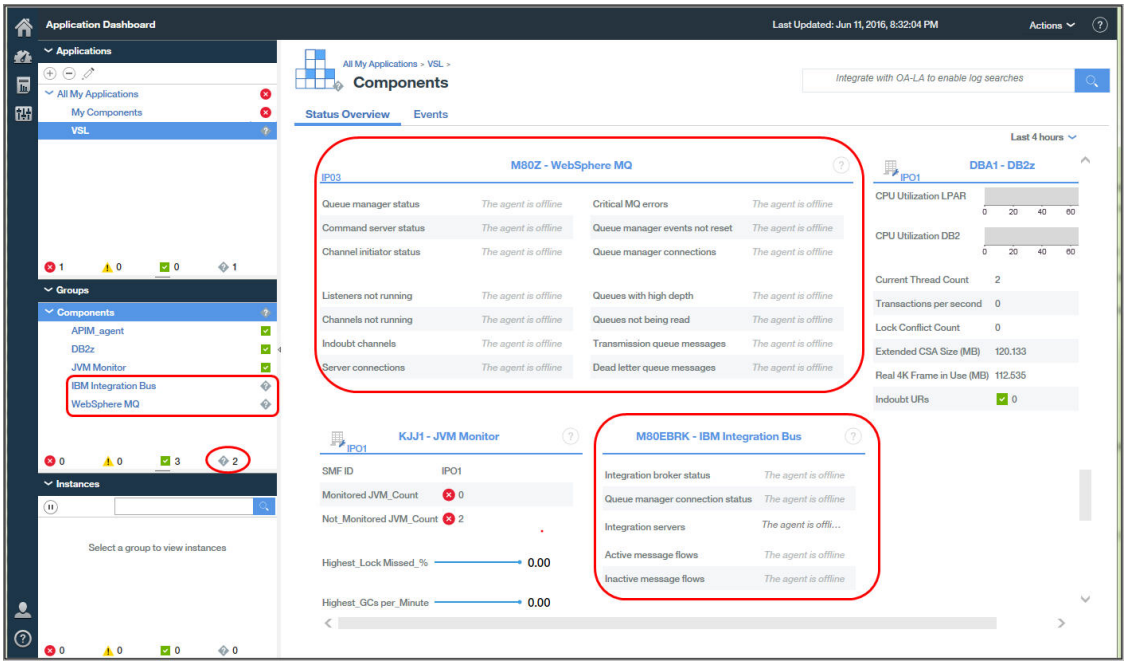
Panel de instrumentos del rendimiento de aplicaciones - Aplicación

Cuando el usuario ha pulsado la barra de título del recuadro de resumen o ha seleccionado la aplicación en el navegador, se visualiza la pestaña **Visión general de estado** con un gráfico **Resumen de gravedad de suceso** vacío. El gráfico de barras **Estado actual de componentes** muestra el estado de los agentes fuera de línea como "Desconocido".



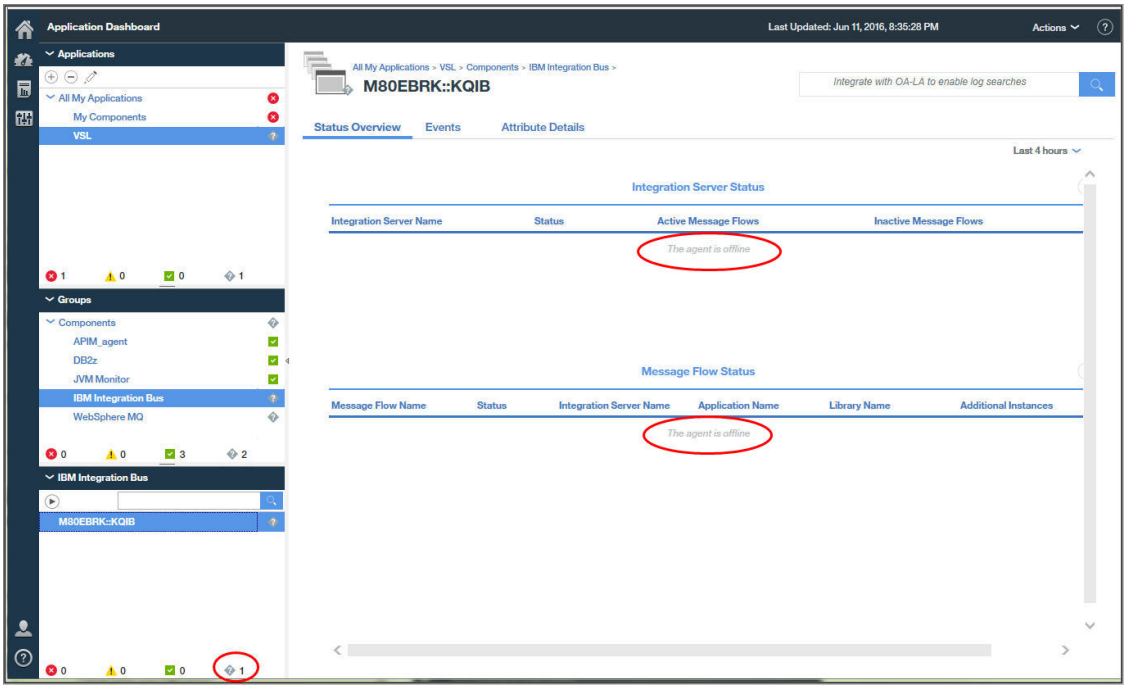
Panel de instrumentos del rendimiento de aplicaciones - Grupo

Cuando el usuario ha pulsado dentro del gráfico **Estado actual de componentes** o el grupo **Componentes** del navegador, la pestaña **Visión general de estado** cambia para mostrar un widget de grupo de resumen para cada uno de los recursos gestionados. Los widgets de grupo para los agentes no disponibles muestran, en lugar de los ICR, un mensaje que indica que el agente está fuera de línea.

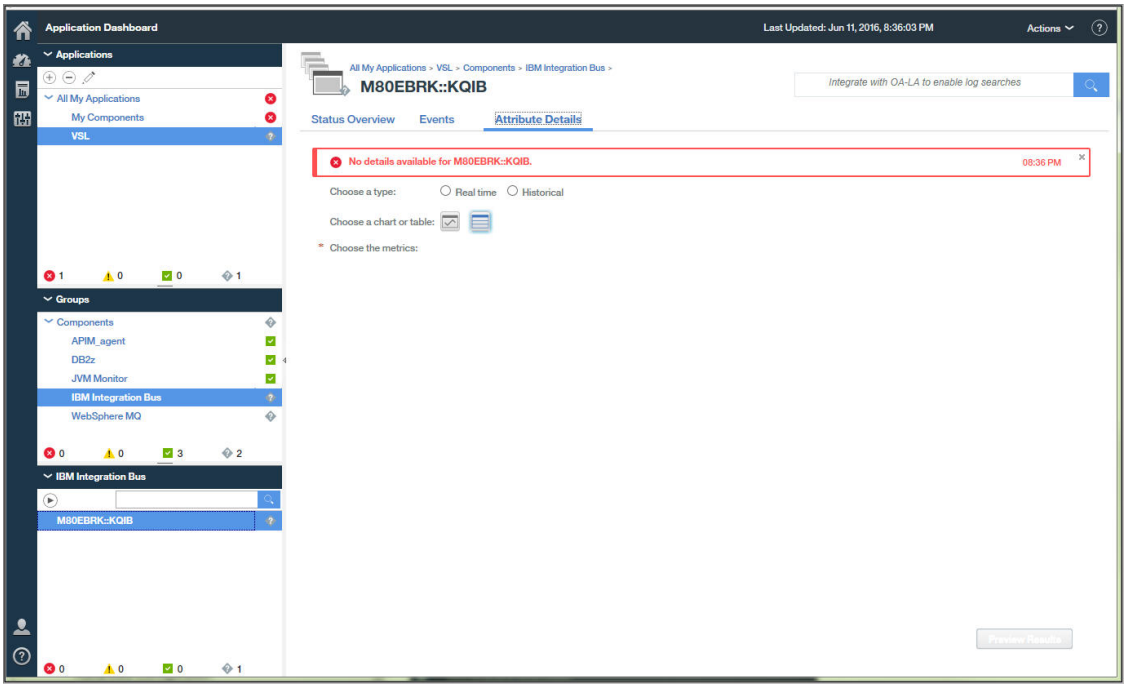


Panel de instrumentos del rendimiento de aplicaciones - Instancia

Cuando el usuario ha pulsado dentro de uno de los widgets de grupo Resumen de agente fuera de línea, la pestaña **Visión general de estado** muestra widgets de gráfico y tabla para el agente seleccionado. Sin embargo, para el widget de grupo Resumen, sólo se muestra un mensaje que indica que el agente está fuera de línea en lugar de los ICR para la instancia de agente.



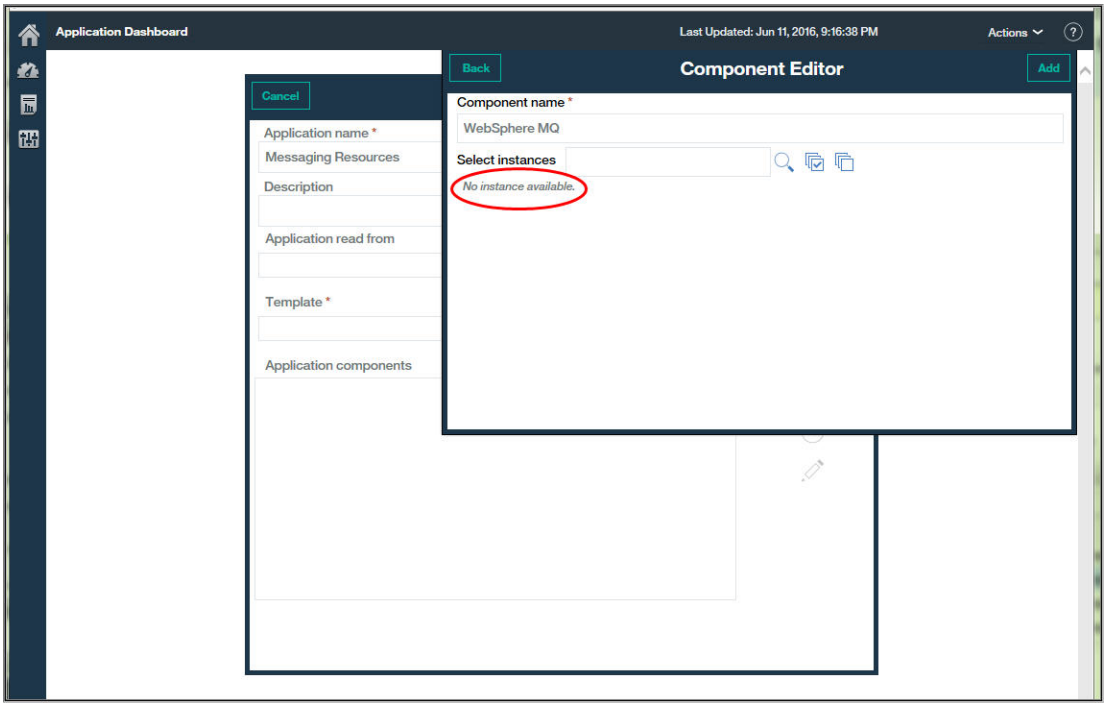
Cuando el usuario ha pulsado la pestaña **Detalles de atributo**, un mensaje indica que no hay detalles disponibles para la instancia de agente. No es posible crear una tabla o un gráfico personalizado para la instancia de agente fuera de línea.



Editor de aplicaciones

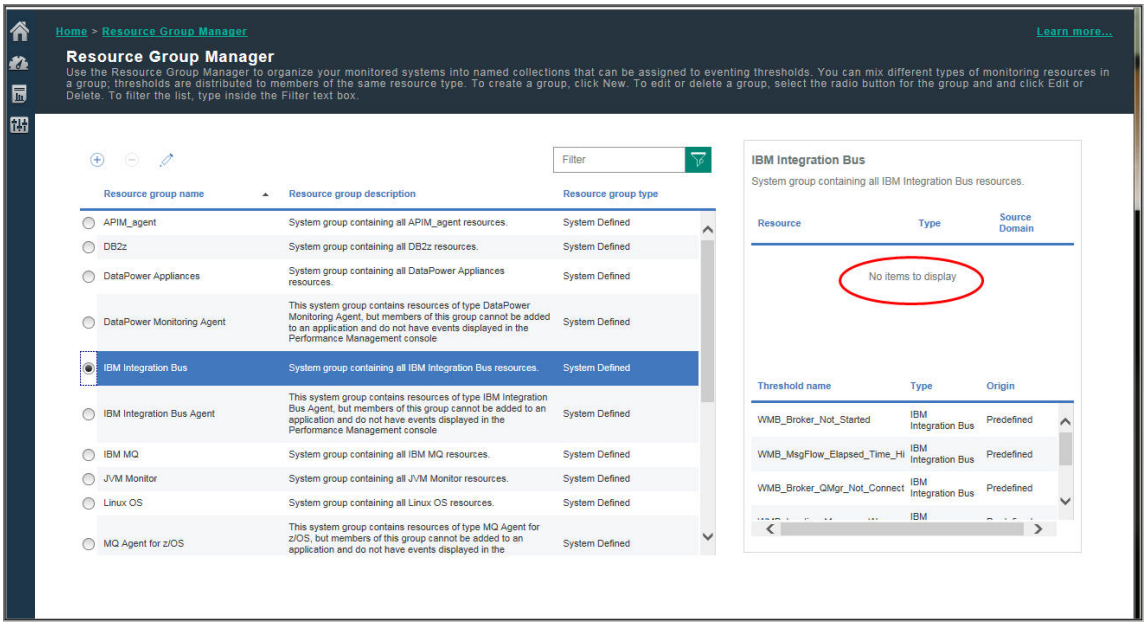
En el Panel de instrumentos del rendimiento de aplicaciones, cuando el usuario ha pulsado la herramienta **Añadir aplicación** o **Editar aplicación** de Aplicaciones del navegador, aparece la ventana del editor de aplicaciones.

Cuando el usuario ha pulsado **Añadir componentes** y ha seleccionado un tipo de agente, si no hay agentes de ese tipo instalados o si están fuera de línea un mensaje indica que no hay instancias de agente disponibles. Si hay otras instancias de agente disponibles, aparecerán en la lista.



Gestor de grupos de recursos

Cuando el usuario ha seleccionado **Configuración del sistema** > **Gestor de grupos de recursos**, la página se abre con una tabla de grupos de recursos. Cuando se selecciona un grupo, sus instancias de agente constituyentes se listan junto con los umbrales asignados. Si todas las instancias de agente están fuera de línea, un mensaje indica que no hay instancias disponibles.



Conceptos relacionados

"Gestión de aplicaciones" en la página 1133
Utilice las herramientas que están disponibles en el Panel de instrumentos del rendimiento de aplicaciones para organizar los recursos gestionados en aplicaciones.

"Utilización de los paneles de instrumentos" en la página 1113

Referencia relacionada

"Gestor de grupos de recursos" en la página 1014
El entorno supervisado puede tener varios sistemas gestionados que se pueden clasificar de acuerdo con su finalidad. Dichos sistemas a menudo tienen los mismos requisitos de umbral. Utilice el **Gestor de grupos de recursos** para organizar sistemas supervisados en grupos a los que puede asignar umbrales. Puede crear también grupos de recursos que se correlacionan con las políticas de control de acceso basado en roles (RBAC).

Estado de suceso

Utilice **Estado de suceso** para obtener una visión general de resumen de sucesos abiertos para el elemento de navegador seleccionado y para responder a sucesos con un estado crítico o de aviso obteniendo más información en los paneles de instrumentos detallados.

Los indicadores de estado son para sucesos de los umbrales que se ejecutan en los sistemas gestionados. Si tiene Pasarelas híbridas configurado, los sucesos también pueden ser de situaciones que se ejecuten en los sistemas gestionados en el entorno de IBM Tivoli Monitoring. Si su configuración incluye IBM Operations Analytics - Predictive Insights, las anomalías detectadas también se visualizan.

Los sucesos para algunos umbrales no se visualizan en Panel de instrumentos del rendimiento de aplicaciones. Los umbrales utilizan atributos para recursos que no están publicados, los cuales se pueden producir en agentes que admiten subnodos. (Para obtener una descripción de los subnodos, consulte el tema Agent Builder,).

Crítico, Aviso, Normal

- Los indicadores de estado consolidan las gravedades de sucesos de los umbrales:

  El estado crítico indica todos los sucesos con una gravedad Muy grave o Crítico

  El estado de aviso indica todos los sucesos con una gravedad Leve o de Aviso

  El estado normal indica todos los sucesos con una gravedad Desconocida

El estado Desconocido indica que el sistema gestionado está fuera de línea. Después de 4 días fuera de línea, el sistema gestionado se elimina de las aplicaciones y ya no se visualiza en los paneles de instrumentos.
Para comprobar el estado, tener o iniciar un agente, consulte "Utilización de mandatos de agente" en la página 184

- V6-V7 Cuando una o varias Pasarelas híbridas están configuradas, los indicadores de estado para los sucesos de situaciones de Tivoli Monitoring son los mismos que para los umbrales excepto que el estado normal indica sucesos con gravedad Inofensivo, Informativo o Desconocido.
- Cuando el entorno gestionado incluye IBM Operations Analytics - Predictive Insights, las anomalías detectadas se indican mediante un icono en forma de rombo sobre el indicador de estado, como, por ejemplo . Para obtener más información, consulte "Investigación de anomalías con Operations Analytics - Predictive Insights" en la página 1146.

Indicador de porcentaje de Resumen de gravedad de suceso

- El indicador Resumen de gravedad de suceso muestra los porcentajes de estado de suceso Crítico, Aviso y Normal. Por ejemplo, 

muestra que el 50% de los sucesos son de umbrales con una gravedad Leve o de Aviso y el 50% son de umbrales con una gravedad Muy grave o Crítica.
- También se informa del número total de sucesos y de cuántos hay para cada nivel de estado.
- El recuento de sucesos incluye las anomalías de Operations Analytics - Predictive Insights. Por ejemplo, un total de "8 incluyendo 1 anomalía" significa que hay 7 sucesos de umbral y 1 suceso de anomalía.

Tabla de sucesos

- La tabla de sucesos abiertos y estados está definida por el elemento de navegador seleccionado: aplicación, grupo, subgrupo o instancia.
- Los sucesos están ordenados por la columna **Gravedad**, apareciendo en primer lugar la gravedad más alta. Pulse la cabecera de una columna para cambiar el orden de clasificación.
- Cada fila proporciona la siguiente información sobre el suceso:

  Nombre de umbral
  El nombre que se ha dado al umbral.

  V6-V7 El nombre otorgado a la situación.

  Estatus
  El estado del suceso, por ejemplo **Abierto**.

  Gravedad
  El valor de la gravedad del suceso: Crítico (se aplica a las gravedades de umbral Muy grave y Crítico), Aviso (se aplica a gravedades de umbral Leve y de Aviso), o Normal (se aplica a las gravedades de umbral Desconocido; para los sucesos de Tivoli Monitoring se aplica a las gravedades Inofensivo, Informativo y Desconocido).

  El estado Desconocido indica que el sistema gestionado está fuera de línea. Después de 4 días fuera de línea, el sistema gestionado se elimina de las aplicaciones y ya no se visualiza en los paneles de instrumentos. (Para comprobar el estado, detener e iniciar un agente, consulte "Utilización de mandatos de agente" en la página 184.)

  Cuando el entorno gestionado incluye IBM Operations Analytics - Predictive Insights, las herramientas de análisis aplicadas a los datos históricos detectan una anomalía y abren sucesos. Un suceso abierto para una anomalía detectada se indica mediante un icono que se superpone al indicador de estado, como por ejemplo . Pulse el enlace **Ver análisis de anomalías** para abrir la vista **Diagnóstico de servicio** de Predictive Insights en una nueva ventana o pestaña del navegador. Utilice la vista **Diagnóstico de servicio** para revisar el comportamiento anómalo en los componentes que dan soporte a la aplicación.

Elemento de visualización
Solo se aplica a conjuntos de datos de varias filas. El elemento de visualización es un atributo clave que se ha seleccionado para que el umbral distinga entre varios sucesos que se han abierto para el mismo sistema gestionado.

Origen
El nombre del host del sistema u otro nombre derivado del agente de supervisión que identifica el origen del suceso.

Indicación de fecha y hora
La fecha y la hora en que el agente originador observó el suceso producido para la condición, expresadas en el huso horario del usuario de la >Consola de Cloud APM.

Si un agente se reinicia o se modifican las definiciones de umbral para un agente, los sucesos muestreados del agente se cierran y reabren si la condición de umbral sigue siendo verdadera. En estos casos, el valor `Indicación de fecha y hora` se actualiza con el valor del momento en que el agente originador reabrió el suceso.

Para sucesos puros, se abre un suceso nuevo por parte del agente que sustituye la instancia de suceso anterior cada vez que el agente de origen determina que la condición de umbral es cierta. Un suceso puro sigue abierto durante 24 horas (o un número de horas configurable) después de la última vez que la condición de umbral se evaluó en true. Solamente se visualiza la instancia más reciente de un suceso puro en Consola de Cloud APM.

Descripción
La descripción, si la hay, que fue escrita para el umbral.

- Pulse en una fila para expandir los detalles sobre el suceso:

Nodo
Nombre del sistema gestionado de la instancia de nodo.

Para los agentes con subnodos, la opción **`Habilitar sucesos de subnodo`** controla si se muestran los subnodos. Para obtener más información, consulte “Integración de interfaz de usuario” en la página 1108.

ID de umbral
El identificador de umbral.

Indicación de fecha y hora global
La fecha y hora en que el Servidor de Cloud APM ha recibido el suceso del agente originador, expresadas en el huso horario del usuario de la Consola de Cloud APM.

Tipo
Si el suceso es puro o de muestra. Los sucesos puros son notificaciones no solicitadas. Los umbrales de los sucesos puros no tienen ningún intervalo de muestreo ni ninguna medida constante que se pueda supervisar para los valores actuales.

Descripción
La descripción, si la hay, que fue escrita para el umbral.

Fórmula
La fórmula tal como se escribe en el Editor de umbrales. Por ejemplo, `Percent Failed > 10.000 AND Transaction Definition Name != 'Ignore_Resources'`.

Si la función Personalización de atributo EIF se ha utilizado para personalizar el valor del atributo base **`msg`**, se visualiza el valor del atributo base **`msg`** personalizado en lugar de la fórmula de umbral. Para obtener más información, consulte “¿Reenviar suceso EIF?” en la página 1020 en el tema del Gestor de umbrales y “Personalización de un suceso para reenviarlo a un receptor EIF” en la página 1025.

Puede seleccionar y ampliar otras filas, o pulsar de nuevo para contraer una fila. Mientras una fila está expandida, puede detallar más en los paneles de instrumentos del sistema gestionado y utilizarlo para ayudar a determinar la causa del suceso.

Investigación de anomalías con Operations Analytics - Predictive Insights

Solo IBM Cloud Application Performance Management: cuando el entorno gestionado incluye IBM Operations Analytics - Predictive Insights, las herramientas de análisis aplicadas a los datos históricos pueden detectar anomalías y abrir sucesos. Utilice el Panel de instrumentos del rendimiento de aplicaciones para ubicar y ver anomalías detectadas por Operations Analytics - Predictive Insights.

Antes de empezar

Operations Analytics - Predictive Insights debe estar integrado con el entorno de Cloud APM para que se le alerte de anomalías en Panel de instrumentos del rendimiento de aplicaciones. Para obtener más información, consulte “Integración con Operations Analytics - Predictive Insights” en la página 1005.

Acerca de esta tarea

La Panel de instrumentos del rendimiento de aplicaciones muestra el resumen de estado de las aplicaciones en los dominios y los sistemas gestionados de sus componentes. Los indicadores de estado de sucesos en los cuadros de resumen del panel de instrumentos **Todas mis aplicaciones** muestran gravedades Crítico, Aviso y Desconocido. Si los sucesos incluyen anomalías detectadas por Operations Analytics - Predictive Insights, el indicador de estado incluye un icono de anomalía: , o . El mismo indicador para las anomalías críticas o de aviso aparece junto al título de pestaña **Sucesos** cuando desciende a mayor nivel en las páginas del panel de instrumentos de aplicaciones, grupos e instancias: Events 2. Para ver una demostración práctica, inicie la IBM Cloud Application Performance Management Demostración guiada, desplácese hacia abajo por la lista de tareas y seleccione *Identificar y diagnosticar anomalías de Predictive Insights*.

Procedimiento

Siga estos pasos para identificar anomalías y verlas en la vista Operations Analytics - Predictive Insights **Diagnóstico de servicio**:

1. Pulse **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** para abrir el panel de instrumentos **Todas mis aplicaciones**.
2. Si un cuadro de resumen tiene un indicador de estado de **Sucesos** que muestra el icono de anomalía, pulse el enlace **Sucesos**.

   El panel de instrumentos de aplicaciones se abre en la pestaña **Sucesos**. **Resumen de gravedad de suceso** informa del número total de sucesos, incluyendo el número de anomalías.
3. Pulse en una fila de la tabla de un suceso anómalo, que se indica en la columna **Gravedad** mediante , o .

   La fila se expande para mostrar los detalles del suceso.
4. Pulse **Ver análisis de anomalías** para abrir la vista **Diagnóstico de servicio** de Operations Analytics - Predictive Insights en una nueva pestaña o ventana de navegador.

Qué hacer a continuación

- Utilice la vista **Diagnóstico de servicio** para revisar el comportamiento anómalo en los componentes que dan soporte a la aplicación. Pulse para abrir la ayuda en línea para la vista **Diagnóstico de servicio**.
- Vuelva al panel de instrumentos de la aplicación y busque otros sucesos del sistema gestionado que puedan indicar un problema relacionado. Pulse la pestaña **Visión general de estado** y profundice en la instancia de sistema gestionado en la que se ha producido el suceso para investigar adicionalmente. Utilice la información para determinar qué acciones deben realizarse para evitar los problemas identificados por Predictive Insights.
- Si espera ver anomalías pero no se visualiza ninguna, es posible que el tiempo de formación de Operations Analytics - Predictive Insights no sea suficiente para generar anomalías. Dos semanas es el tiempo de formación típico. También es posible que sea necesaria configuración adicional.

Vistas personalizadas

Utilice la IBM Cloud Application Business Insights Universal View para aumentar el valor que ya proporcionan las páginas predefinidas del Panel de instrumentos del rendimiento de aplicaciones personalizando sus propias páginas.

Universal View se puede utilizar para visualizar datos de supervisión de recursos. No se puede utilizar para visualizar datos de transacciones sintéticas, datos de rastreo de transacciones, datos de agente de tiempo de respuesta y datos de diagnóstico en profundidad. Mediante la Universal View, puede crear rápidamente páginas de supervisión para una aplicación y guardarlas para visualizarlas. Al visualizar una página del panel de instrumentos personalizada guardada, puede ver el panel de instrumentos en modalidad de renovación automática, exportarlo en un archivo de datos en bruto, editarlo o suprimirlo.

Los cuatro roles predeterminados de Cloud APM: Administrador de roles, Administrador de supervisión, Administrador del sistema y Usuario de supervisión tienen permisos diferentes para ver y modificar páginas de panel de instrumentos. Para obtener más información, consulte Tabla 1. Roles y permisos .

Las opciones que están disponibles en la pestaña **Vistas personalizadas** dependen de si la página se está editando o visualizando.

Creación y gestión de páginas personalizadas

Utilice la pestaña Vistas personalizadas para crear o editar páginas de paneles de instrumentos para la aplicación, grupo o instancia seleccionada añadiendo o actualizando widgets que se llenan con las métricas de recursos de su elección.

Acerca de esta tarea

Las páginas que crea y guarda se asocian a la aplicación seleccionada. Por ejemplo, la aplicación Gestión de inventario de la Demostración guiada de Cloud APM tiene los agentes de supervisión siguientes: Linux OS, MySQL, Node.js, Hadoop y Ruby. Puede crear y guardar una página personalizada en cualquier nivel del navegador desde aplicación a instancia y a continuación abrirla en el mismo nivel en el que se ha creado. Una página que se crea en un nivel determinado sólo puede abrirse en el mismo nivel. Las métricas disponibles para los widgets pueden ser de cualquiera de los recursos de la aplicación. Con el ejemplo de Gestión de inventario, puede crear una página con una tabla del Agente de Ruby, un gráfico del Agente de sistema operativo Linux, etc.

Procedimiento

Las páginas que crea y guarda se asocian a la aplicación seleccionada. Complete los pasos siguientes para crear y personalizar una página del panel de instrumentos:

1. Después de abrir el Panel de instrumentos del rendimiento de aplicaciones desde el menú **Rendimiento**, seleccione una aplicación.

   La pestaña **Vistas personalizadas** se visualiza después de las pestañas **Visión general de estado** y **Sucesos**. También puede avanzar al nivel de grupo, subgrupo o instancia del navegador.
2. Pulse la pestaña **Vistas personalizadas**.

   La pestaña muestra la ventana **Seleccionar una plantilla para la página personalizada**, o la página predeterminada si ya hay una página predeterminada establecida.

   - Si se abre la ventana **Seleccionar una plantilla para la página personalizada**, vaya al paso 4.
   - Si se visualiza la página predeterminada, vaya al paso 3.
3. Pulse **Añadir** para crear una página nueva.
4. Pulse una plantilla de las opciones de plantilla predeterminadas siguientes:

   - Plantilla 1x1
   - Plantilla 1x2
   - Plantilla 2x2

- Plantilla 2x3
- Plantilla 3x3
- Plantilla 3x2
- Plantilla 2x1
- Plantilla 1x3
- Plantilla 3x1

Si pulsa **Atrás**, se abrirá la página marcada como favorita o la primera página de la lista. Si no existe ninguna página, se abre la ventana **Seleccionar una plantilla para la página personalizada**.

5. Personalice la plantilla. Si desea obtener más información, consultePersonalización de plantillas.
6. Cree un a widget. Si desea obtener más información, consulte"Definición de propiedades de widget" en la página 1151.
7. Pulse  **Establecer marco de tiempo predeterminado de página** y establezca el período de retención de datos predeterminado para la página en 1, 2, 4, 12 o 24 horas.
8. Cuando esté preparado para guardar la página, siga estos pasos:
   a) En el campo **Nombre de página**, especifique el nombre de la página.

      Importante: En el campo **Nombre de página** se permiten espacios, signos de subrayado (_) y guiones (-). Sin embargo, no se permite un guión seguido de un signo de subrayado (-_). Por ejemplo, no se permite `System-_Overview`.

   b) Pulse **Guardar**.

      Los cambios siguientes se pueden producir en el panel de instrumentos o puede aparecer el mensaje:

      - Se visualizará el mensaje `Panel de instrumentos guardado`.
      - Si se selecciona ***** en **Establecer condiciones**, se visualizará el siguiente mensaje:

        ```
        Ha seleccionado * en Instancia de recurso o en Establecer condiciones,
        lo que provocará una gran cantidad de datos (como, por ejemplo, líneas
        de un gráfico). La gran cantidad de series de datos puede provocar que
        no la página no se pueda leer o que el rendimiento sea inutilizable. El
        límite aconsejado para este gráfico es de 50 series de datos. La adición
        de valores específicos ayuda a precisar los datos en los límites y
        resultados recomendados consiguiendo una mejor experiencia para el
        usuario.
        ```

      - Aparece un indicador de color rojo en el  para indicar que no se ha seleccionado el tipo de gráfico y que se debe seleccionar.
      - Aparece un indicador de color rojo en el  para indicar que no se ha seleccionado la opción Seleccionar métricas y que se tiene que seleccionar y, a continuación, se visualizará el mensaje siguiente:

        ```
        Se tiene que guardar una métrica para guardar un gráfico.
        ```

9. Seleccione cualquiera de las opciones siguientes en la barra de título de la página:

Opción	Descripción
 **Recuperar tipos de métrica de recurso más recientes**	Pulse para renovar los tipos de métrica. Si se ha producido un cambio en el tipo de métrica o en la métrica cuando se aplica cualquier parche de agente, debe renovar los tipos de métrica. El intervalo entre dos renovaciones queda restringido a 15 minutos. Si pulsa  **Recuperar tipos de métrica de recurso más recientes**

Opción	Descripción

	dentro de los 15 minutos siguientes a la renovación anterior, se visualiza el mensaje siguiente:
	`La memoria caché de metadatos se ha renovado recientemente. Espere` *`tiempo_restante`* `minuto(s) a que se vuelva a cargar.`
	Mientras se cargan los metadatos, se visualiza una imagen de carga.
	Cuando se han cargado los metadatos, se visualiza el mensaje siguiente:
	`La memoria caché de metadatos se ha vuelto a cargar satisfactoriamente.`
	Si la renovación de los metadatos tarda más de 30 segundos, se visualiza el mensaje siguiente:
	`La recarga de la memoria caché de metadatos puede tardar algún tiempo.`
	`¿Todavía desea esperar a que se lleve a cabo?`
	Puede pulsar **Aceptar** o **Cancelar**.

 **Ver panel de instrumentos**	Púlselo para ver los datos en el panel de instrumentos. **Importante:** El límite para el número de filas que se devuelven por definición de datos es de 11.000 filas. De forma predeterminada, se visualizarán los datos más recientes cuando se cruce el límite. Para los volúmenes grandes de datos, no se visualizan todos los datos del intervalo de tiempo seleccionado. Por ejemplo, si selecciona ver los datos de las últimas 24 horas para un origen de datos de gran volumen, puede que solamente se visualicen las últimas 6 horas de datos si se ha alcanzado el límite de 11.000 filas. Si en un gráfico se supera la cifra de 50 series de datos, se visualizará el siguiente mensaje en el widget: `Este gráfico no se puede cargar porque la cantidad de series de datos (como, por ejemplo, líneas en un gráfico) supera los 50. La cifra de series de datos es actualmente` *`series_datos_actual`*`. Puede reducir la cantidad seleccionando menos métricas o instancias de recursos, o precisando las Condiciones por métrica. Para obtener más información, consulte Definición de las propiedades de widget: para Cloud APM, http://ibm.biz/widgetprops y para Cloud APM Private, http://ibm.biz/widgetprops-private` Si un gráfico tarda más de 30 segundos en cargarse, se visualizará el siguiente mensaje en el widget: `Este gráfico tarda demasiado en cargarse debido a un problema por una gran cantidad de datos, una latencia de red larga o un problema de conectividad. Reduzca la cantidad de instancias de recursos o precise las condiciones por métrica para acotar los datos. Para obtener más información, consulte Definición de las propiedades de widget: para Cloud APM, http://ibm.biz/widgetprops y para Cloud APM Private, http://ibm.biz/widgetprops-private`

Opción	Descripción
Guardar como	Pulse la flecha situada junto a **Guardar** y pulse **Guardar como** y especifique un nombre diferente en el campo **Nombre de página** para guardar la página con un nombre diferente. **Importante:** Si especifica un nombre de página que coincide con una página existente, se sobrescribe la página existente.
Suprimir	Púlselo para suprimir la página actual.
Back **Atrás**	Púlselo para volver a la página anterior o a la página favorita.

Qué hacer a continuación
Vea las páginas personalizadas tal como se describen en "Visualización de páginas personalizadas" en la página 1154.

Personalización de plantillas
Puede personalizar la plantilla redimensionándola, moviéndola o añadiendo marcadores de posición de widget según sus necesidades.

Acerca de esta tarea

Recuerde: Puede personalizar una plantilla existente y utilizarla. Pero la plantilla personalizada no se puede guardar para un próximo uso con el fin de crear paneles de instrumentos nuevos.

Procedimiento

1. En la pestaña Vistas personalizadas, pulse **Editar plantilla**.
2. Seleccione un marcador de widget.
   Puede redimensionar un marcador de widget desde todos los lados y arrastrarlo a una ubicación diferente. Si los widgets se solapan entre sí al redimensionarlos o arrastrarlos, se visualiza el mensaje `Operación de redimensionamiento no válida` u `Operación de movimiento no válida`.
3. Para añadir un marcador de widget a una plantilla existente, realice los pasos siguientes:
   a) Pulse **Establecer altura de página** en las opciones de menú y especifique un valor mayor para el recuento de filas y pulse en cualquier lugar fuera del menú para aumentar la altura de la página.
   b) Especifique un marcador de widget según sus necesidades en el área en blanco de la página colocando el puntero y arrastrándolo para crear un recuadro.
4. Utilice las siguientes opciones de menú para realizar diferentes operaciones en la plantilla:

Opción	Descripción
Deshacer	Para deshacer la última acción.
Rehacer	Para rehacer la última acción.
Suprimir recuadro seleccionado	Para suprimir un widget, selecciónelo y pulse **Suprimir recuadro seleccionado**.
Restablecer	Para crear una plantilla en blanco. Para especificar un marcador de widget en la plantilla en blanco, sitúe el puntero sobre el área Dibujar plantillas aquí y arrástrelo para crear un recuadro. Puede crear marcadores de widget de diferentes tamaños en el área Dibujar plantillas aquí. Los marcadores se pueden mover o redimensionar, pero no solaparse entre sí.

Opción	Descripción
Establecer altura de página	Para establecer la altura de la página. Puede especificar un número de filas de 20 a 120 filas.

5. Pulse **Editar plantilla** para utilizar la plantilla que se crea.

Qué hacer a continuación
Cree el widget. Vaya al paso 6 del tema Creación y gestión de páginas personalizadas.

Definición de propiedades de widget
Defina propiedades diferentes para los widgets, como métricas y gráficos, para ver datos en tiempo real en los widgets.

Procedimiento

Para definir las propiedades de un widget, siga estos pasos:

1. En un widget, pulse para seleccionar un tipo de gráfico para visualizar datos.
   - Línea
   - Área
   - Barra
   - Cuadrícula

   Importante: Para gráficos de líneas, área y barras, si hay más de nueve leyendas, el color del gráfico se repite a partir de la novena leyenda. El color del gráfico es el mismo para la primera y la décima leyendas, para la segunda y la decimoprimera, etc.

   El indicador verde se visualiza en el para indicar que se ha seleccionado ese tipo de gráfico.
2. Especifique las siguientes propiedades de gráfico para los gráficos de líneas, área y barras:
   - Etiqueta del eje X
   - Etiqueta del eje Y
   - Mostrar leyenda
   - Mostrar interpolación: los datos recopilados que deben trazarse en el gráfico, que pueden incluir algunos valores nulos. Por tanto, cuando se traza el gráfico, la línea gráfica se desconecta cuando encuentra un valor nulo y en el gráfico aparecen varias líneas desconectadas. Si selecciona interpolación, la línea del gráfico no aparece desconectada cuando encuentra un valor nulo, sino que se conecta al siguiente valor válido disponible. Por tanto, si selecciona interpolación, obtendrá una única línea gráfica conectada.

     Nota: Para APM V8.1.4.0 IF0005 y versiones posteriores, los gráficos de líneas y barras ya no muestran las líneas desconectadas para valores nulos. Por lo tanto, la característica Mostrar interpolación ya no se requiere y, por lo tanto, no está soportada.

   Importante: La cuadrícula no tiene propiedades.
3. Pulse para seleccionar el contenido de la métrica.

Opción	Descripción
Tipo de recurso	En la lista **Tipo de recurso**, seleccione un recurso. Los recursos disponibles están asociados con la aplicación. Si un recurso que forma parte de la aplicación no está disponible en la lista, significa que no se ha encontrado su definición de recurso. La definición de recurso no se ha publicado o el sistema gestionado no está conectado con el Servidor de Cloud APM.

Opción	Descripción
Tipo de métrica	En la lista **Tipo de métrica**, seleccione un conjunto de datos que desee incluir en el widget.
Medida	En la lista **Medida**, seleccione un atributo para incluirlo en la vista. Los atributos disponibles proceden del conjunto de datos seleccionado. Para seleccionar la medida, siga estos pasos: a. Pulse la lista **Medida**. Se abre una ventana emergente donde las medidas aparecen por orden alfabético clasificadas en orden ascendente. b. Pulse los atributos que se listan en Medidas (seleccione uno o varios) o pulse **Seleccionar todo**. **Nota:** Cuando pulse **Seleccionar todo**, se seleccionarán todas las medidas de la lista. c. Pulse  para añadir las medidas en la lista **Medidas seleccionadas**. d. Si desea suprimir una medida de **Medidas seleccionadas**, pulse  . e. Pulse la lista **Instancia de recurso** para cerrar la ventana emergente. **Importante:** Para gráficos de líneas, barras y áreas, es necesario seleccionar una métrica que contenga un valor numérico. Las métricas que contienen valores de serie no se pueden visualizar en estos gráficos. **Consejo:** Para obtener una cuadrícula, limite su selección a las medidas en función de la salida que se adapte a la visibilidad de la interfaz de usuario.
Instancia de recurso	Inicialmente la selección es *, que recupera las métricas de todas las instancias de la lista. Conserve el valor predeterminado o seleccione la instancia en la lista. **Importante:** Si selecciona una instancia, este widget no puede utilizarse para visualizar datos para ningún otro agente o instancia. Sin embargo, es aconsejable especificar la instancia para evitar el proceso de datos grandes.
Establecer condición para grupo de métricas	Si el **Tipo de métrica** seleccionado tiene varios elementos, como por ejemplo CPUs o discos, **Establecer condición para grupo de métricas** visualizará otros elementos que podrá seleccionar en el campo **WHERE**. **Importante:** Especifique valores para los elementos en el campo **WHERE**. Evite especificar ***** para reducir el proceso de datos grandes. De forma predeterminada, la condición WHERE muestra las últimas 4 horas de datos. Este intervalo de tiempo lo puede cambiar el administrador del sistema entre 1 y 24 horas. Consulte "Cambio del intervalo de tiempo para los datos de la condición WHERE" en la página 1153.
Acciones	Pulse  **Guardar** para guardar una métrica.

Opción	Descripción
	Pulse **Editar** para editar una métrica. Pulse **Suprimir** para suprimir una métrica.

4. Para añadir otra métrica, pulse **+ Añadir otra métrica**.

   Importante: No se aplica a la cuadrícula.
5. Cierre la ventana **Seleccionar métricas** después de añadir todas las métricas.

   Todas las métricas se guardarán automáticamente después de cerrar la ventana **Seleccionar métricas**.

   Los cambios siguientes se pueden producir en el panel de instrumentos o puede aparecer el mensaje:

   - Si se ha seleccionado ***** en la lista **Instancia de recurso** en alguna de las medidas, se visualizará el mensaje siguiente:

     ```
     Ha seleccionado * en Instancia de recurso o en Establecer condiciones, lo
     que provocará una gran cantidad de datos (como, por ejemplo, líneas de un
     gráfico). La gran cantidad de series de datos puede provocar que no la
     página no se pueda leer o que el rendimiento sea inutilizable. El límite
     aconsejado para este gráfico es de 50 series de datos. La adición de
     valores específicos ayuda a precisar los datos en los límites y resultados
     recomendados consiguiendo una mejor experiencia para el usuario.
     ```

   - Aparece un indicador de color verde en  para indicar que las medidas se han seleccionado correctamente para precisar los datos en los límites recomendados.

   - Aparece un indicador naranja en  para indicar que las medidas no se han seleccionado correctamente para precisar los datos en los límites recomendados. O se ha seleccionado ***** en **Instancia de recurso** o en **Establecer condiciones**.

6. Pulse  para especificar el título del widget.

   Si el título del widget no se añade, se asignará automáticamente el nombre de la primera métrica como título del widget.

Qué hacer a continuación

De modo similar, puede añadir gráficos, métricas y títulos a todos los widgets y luego ir al paso 7 del tema Creación y gestión de páginas personalizadas.

Cambio del intervalo de tiempo para los datos de la condición WHERE

El administrador del sistema puede cambiar intervalo de tiempo entre 1 y 24 horas.

Procedimiento

Para cambiar el intervalo de tiempo, el administrador del sistema puede completar los pasos siguientes:

1. Inicie sesión en el servidor APM donde se ha desplegado la compilación.
2. En la línea de mandatos, ejecute los mandatos siguientes:

   ```
   export CLASSPATH=$CLASSPATH:/dir_instalación/gaian/lib/derbytools.jar:
   export CLASSPATH=$CLASSPATH:/dir_instalación/gaian/lib/derbyclient.jar:
   export CLASSPATH=$CLASSPATH:/dir_instalación/gaian/lib/derby.jar:
   java org.apache.derby.tools.ij
   connect 'jdbc:derby://localhost:puerto/
   gaiandb;user=gaiandb;password=contraseña_bd_gaian;';
   ```

En estos mandatos, *dir_instalación* hace referencia al directorio donde se ha desplegado APM, de forma predeterminada es `/opt/ibm`. En el mandato **connect**, *puerto* se refiere al valor del puerto en el que se ha configurado la base de datos, y *contraseña_bd_gaian* es la contraseña de la base de datos Gaian. Póngase en contacto con el soporte de IBM para obtener esta contraseña.

3. Una vez conectada la base de datos, ejecute la consulta siguiente para modificar los valores del intervalo de tiempo:

   ```
   UPDATE "OED_TOOL"."PREFERENCETABLE" SET PREFERENCES='-24H' WHERE
   FIELD='TIMEINTERVAL';

   Commit;

   Exit;
   ```

   Aquí el valor del intervalo de tiempo se ofrece en `SET PREFERENCES='-24H'`. Se puede establecer entre 1H y 24H.

Visualización de páginas personalizadas

Después de crear y guardar páginas de panel de instrumentos para una aplicación, grupo, subgrupo o instancia en la pestaña **Vistas personalizadas**, puede verlas en cualquier momento. Algunas de las opciones que puede seleccionar incluyen renovar la página, seleccionar un intervalo de tiempo diferente, editar la página para recuperar datos de recursos diferentes y exportar el panel de instrumentos como un archivo de datos sin formato.

Procedimiento

Siga estos pasos para ver una página guardada en la pestaña **Vistas personalizadas** del panel de instrumentos.

1. Después de abrir el Panel de instrumentos del rendimiento de aplicaciones desde el menú **Rendimiento**, seleccione una aplicación.

   La pestaña **Vistas personalizadas** se visualiza después de las pestañas **Visión general de estado** y **Sucesos**. También puede avanzar al nivel de grupo, subgrupo o instancia del navegador.
2. Seleccione la pestaña **Vistas personalizadas**.

   La pestaña muestra la ventana **Seleccionar una plantilla para la página personalizada**, o la página predeterminada si ya hay una página predeterminada establecida.
3. Pulse en la lista de páginas y seleccione una de las páginas guardadas de la lista.

   Las páginas disponibles han sido guardadas por usted o las ha compartido otro usuario.

   Después de seleccionar una página guardada, las muestras de datos actuales e históricos se notifican en la página.
4. Seleccione cualquiera de las opciones de visualización en la barra de título de la página:

Opción	Descripción
Renovar	Indica que la renovación automática está desactivada. Pulse para activar la renovación automática.
Renovar	Indica que la renovación automática está activada. Pulse para desactivar la renovación automática. **Importante:** El tiempo de renovación predeterminado es 1 minuto.
Exportar > Datos en bruto	Pulse para exportar la página como formato DAT. Dado que se exportan varios archivos DAT, se descargan en el sistema en formato ZIP. **Recuerde:** Si el archivo descargado no tiene ninguna extensión, añádale zip como extensión.

Opción	Descripción
	Importante: Si el archivo no se ha descargado en el sistema, compruebe si el software para bloquear ventanas emergentes está habilitado. Puede añadir este sitio a su lista de excepciones. Extraiga el archivo ZIP descargado. Los archivos extraídos son archivos de texto sin formato. El archivo contiene el nombre de la página, duración, filtros, fecha, hora, intervalo, título del gráfico y datos. El delimitador de datos es la barra vertical. Puede abrir los archivos DAT mediante el editor adecuado o importarlos en Excel especificando los separadores de valor adecuados.
 **Exportar > PDF**	Pulse para exportar la página como formato PDF. El archivo contiene el nombre de página, el intervalo de tiempo, los widgets, el valor creado por y el informe de creación.
 **Editar**	Púlselo para editar la página actual. Puede cambiar los gráficos y métricas de los widgets, añadir nuevos widgets o cambiar el marco temporal predeterminado o editar el nombre para la página.
 **Suprimir**	Púlselo para suprimir la página actual.
 **Añadir**	Púlselo para crear una página nueva. Para personalizar la página y guardarla, consulte “Creación y gestión de páginas personalizadas” en la página 1147.

5. Seleccione cualquiera de las opciones de visualización siguientes en el widget:

Opción	Descripción
 **Tipo de gráfico**	Pulse el icono **Tipo de gráfico** y seleccione una opción adecuada de la lista para cambiar el tipo de gráfico existente. • Para gráficos de líneas y áreas, dispone de las opciones **Líneas** y **Áreas**. • Para gráficos de barras, dispone de las opciones **Barras agrupadas** y **Columnas agrupadas**. **Importante:** Para cuadrícula, no hay opciones de tipo de gráfico. Para los datos visualizados en una cuadrícula, puede filtrar los datos de la siguiente manera: a. Pulse  **Definir filtro**. Se abrirá la ventana **Filtrar**. b. Especifique valores para **Columna**, **Condición** y **Valor** para añadir una regla de filtro. **Nota:** Puede filtrar los valores numéricos y los valores de texto seleccionando las condiciones adecuadas. c. Pulse  **Añadir regla de filtro** para añadir otra regla de filtro. Puede añadir varias reglas de filtro.

Opción	Descripción
	d. En el campo **Coincidencia**, seleccione **Todas las reglas** o **Cualquier regla** para filtrar los datos. Puede seleccionar **Coincidencia de mayúsculas/minúsculas** si desea buscar en función de las mayúsculas y minúsculas del texto que especifique en el campo **Valor**. e. Pulse **Filtrar** para filtrar los datos que se muestran en la cuadrícula. f. Pulse **Borrar filtro** para borrar los resultados del filtro. g. Pulse **cancelar** para cerrar la ventana **Filtrar**.
Contraer	Púlselo para contraer el widget.
Expandir	Púlselo para expandir el widget.
Maximizar	Púlselo para maximizar el widget al tamaño de la página.
Restaurar	Púlselo para restaurar el widget a su tamaño original.
Leyendas	El widget contiene recuadros de selección para cada métrica. Marque o quite la marca de los recuadros de selección para cada métrica para ver los datos de una métrica concreta o de varias métricas.

6. Puede filtrar los datos en la página utilizando las listas **Fecha**, **Hora** e **Intervalo**. También puede definir un filtro personalizado para que la página muestre datos para los intervalos de fecha y hora seleccionados. Para utilizar el filtro personalizado, en la lista **Intervalo**, seleccione **Personalizado** y, a continuación, en la ventana **Selección de periodo de tiempo**, seleccione los intervalos de fecha y hora necesarios.

   Nota:

   - La opción de filtro personalizado está disponible a partir de APM V8.1.4.0 IF0005. Las páginas creadas con versiones anteriores de Cloud APM no muestran la opción Filtro personalizado.
   - Utilice Filtro personalizado para filtrar datos para un intervalo de tiempo mínimo de 1 minutos y un intervalo de tiempo máximo de 24 horas.
   - Al aplicar un filtro personalizado, en la ventana **Selección de periodo de tiempo**, si pulsa **Cancelar**, a continuación en la página del panel de instrumentos la lista **Intervalo** no mostrará el intervalo que ha aplicado anteriormente.
   - Si aplica el filtro personalizado a una página, los datos de la página no se renovarán automáticamente.

7. Para establecer una página predeterminada, pulse en la página y pulse  **Favorito** junto al nombre de la página que desea establecer como la página predeterminada.

Programas de utilidad del panel de instrumentos

Utilice las opciones disponibles para gestionar el aspecto y comportamiento de las páginas de **Panel de instrumentos del rendimiento de aplicaciones**.

Copia del URL del panel de instrumentos

Después de navegar a un lugar de la jerarquía de aplicaciones, el URL del recuadro de dirección del navegador no cambia para la nueva vista. Puede copiar el URL de la página de Panel de instrumentos del rendimiento de aplicaciones que está visualizando. Pegue el URL en una nueva ventana de navegador

para abrir la página del panel de instrumentos o utilice el URL para acceder al panel de instrumentos más adelante o para compartir con otros.

Procedimiento

1. Vaya a la página de Panel de instrumentos del rendimiento de aplicaciones que desea recordar.
2. Pulse **Acciones** > **Copiar URL**.
3. Pulse el botón derecho del ratón en el enlace de hipertexto **Enlace a la página actual** y seleccione la opción para copiar el URL.

Qué hacer a continuación
Guarde una copia del URL o compártala con otros usuarios en su entorno gestionado. Después de pegar el URL en el recuadro de dirección del navegador, la página del panel de instrumentos de destino se abre en la Consola de Cloud APM.

Si no ha iniciado la sesión en el Servidor de Cloud APM, se le solicitará que especifique el ID de usuario y la contraseña antes de que se pueda visualizar la página del panel de instrumentos de destino. Si se abre la página **Cómo empezar** en lugar de la página del panel de instrumentos, pulse F5 o pulse el botón de renovación en la barra de herramientas del navegador. Puede desactivar la página **Cómo empezar** para sesiones de trabajo futuras deseleccionando el recuadro "Mostrar esta página **Cómo empezar** en el inicio".

Configuración de un rastreo

Ajuste los valores de rastreo para ayudar al administrador o al servicio de soporte de IBM a diagnosticar la causa de los problemas mediante el Panel de instrumentos del rendimiento de aplicaciones.Hay disponibles varios niveles de rastreo mientras trabaja con el navegador y la pestaña **Visión general de estado**. Puede iniciar un nivel de rastreo detallado exactamente en el punto en la interfaz de usuario donde está teniendo un problema y, a continuación, volver el rastreo a un nivel reducido después de capturar los datos de registro necesarios. Por ejemplo, si un determinado panel de instrumentos se comporta de forma inesperada, puede elevar el nivel de rastreo antes de abrir el panel de instrumentos para registrar la actividad y, a continuación, volver a establecer el registro de rastreo al nivel normal.

Acerca de esta tarea
Realice los pasos siguientes para establecer el nivel de rastreo cuando desee aumentar o reducir la cantidad de registro de rastreo.

Procedimiento

1. Si el Panel de instrumentos del rendimiento de aplicaciones no está abierto, selecciónelo en la opción **Rendimiento** en la barra de navegación.
2. Seleccione Todas mis aplicaciones o una aplicación en el navegador o en la pestaña Visión general de estados.
3. Pulse **Acciones** > **Nivel de rastreo** y seleccione uno de los niveles siguientes:
   - **Detallado** para registrar toda la actividad. El nivel de rastreo detallado incluye registro de rastreo Moderado, Ligero y Mínimo.
   - **Moderado** permite registrar cambios de variables, como por ejemplo, los parámetros proporcionados y los cálculos realizados. El nivel de rastreo Moderado incluye el registro de rastreo Ligero y Mínimo.
   - **Ligero** permite registrar actividad de errores y variables. Es posible que desee establecer el rastreo en este nivel si tiene problemas tales como que no se devuelven datos pero el panel de instrumentos sigue funcionando. El nivel de rastreo Ligero incluye el registro de rastreo Mínimo.
   - **Mínimo** es el valor predeterminado y sólo registra los errores irrecuperables. Puede volver a establecer el nivel de rastreo a mínimo después de recopilar una secuencia de actividad específica. Aunque se establezca un nivel de rastreo diferente antes de cerrar la sesión, siempre se restablecerá al valor más bajo la próxima vez que inicie sesión.

4. Si desea enviar registros de rendimiento a un archivo de registro común, seleccione **Habilitar de registro de estadísticas de rendimiento**.

   La información de rendimiento de la consola se escribe en el servidor donde puede combinarse con las estadísticas de rendimiento del servidor para proporcionar el tiempo de respuesta de transacciones global. La información de rendimiento necesaria incluye la hora de inicio de una función y la hora en que termina.

Resultados

El rastreo se ajusta al nivel elegido. La próxima vez que inicie la sesión, el rastreo estará en **Mínimo** hasta que lo cambie de nuevo.

Para minimizar el tráfico de las comunicaciones, los mensajes de registro se transfieren por lotes. Después de cerrar la sesión, se realiza una transferencia final, ya sea manualmente o después de un periodo de tiempo de espera. (Si el navegador falla, no se envía ningún registro final). El registro se guarda en el servidor y se llama `itp.log`. Se crea un `itp.log` nuevo cada vez que se reinicia el servidor.

Si establece **Habilitar registro de estadísticas de rendimiento**, se guardan registros similares a los del ejemplo siguiente en *dir_instalación*`/usr/servers/apmui/logs/itp.log`:

```
<record>
    <date>2013-10-02T10:52:46</date>
    <millis>1380736366788</millis>
    <sequence>28008</sequence>
    <level>INFO</level>
    <class>StatusItemList</class>
    <method>tracing</method>
    <thread>96</thread>
    <message>BeginTrace:onSelectApp:272wt877d05</message>
</record>
<record>
    <date>2013-10-02T10:52:46</date>
    <millis>1380736366809</millis>
    <sequence>28009</sequence>
    <level>INFO</level>
    <class>StatusItemList</class>
    <method>tracing</method>
    <thread>96</thread>
    <message>EndTrace:onSelectApp:272wt877d05</message>
</record>
```

Bloqueo de la Consola de Cloud APM

Puede bloquear temporalmente la sesión de trabajo sin tener que finalizar sesión en la Consola de Cloud APM. La característica de bloqueo de sesiones no está disponible en Apple iPad.

Procedimiento

1. Una vez que ha iniciado la sesión en Consola de Cloud APM, pulse ***apmadmin*** > **Bloquear sesión**, donde *apmadmin* es el nombre que ha utilizado para iniciar la sesión.

   Se visualiza la pantalla de inicio de sesión y la sesión se bloquea.
2. Para desbloquear la sesión, escriba la contraseña para el ID de usuario.

   La sesión de trabajo se reanuda.

Informes

En la Consola de Cloud APM hay informes históricos disponibles para los datos recopilados por el Agente de Supervisión de tiempo de respuesta, el Agente de WebSphere Applications y el Agente de Synthetic Playback.

Puede ejecutar informes desde el panel de instrumentos **Todas mis aplicaciones**. Desde cualquier página de Consola de Cloud APM, pulse **Rendimiento** > **Panel de instrumentos del rendimiento de aplicaciones** para abrir el panel de instrumentos **Todas mis aplicaciones**.

Nota: La primera vez que ejecute un informe, debe iniciar la sesión en Tivoli Common Reporting como un usuario que tenga permiso para ejecutar informes de Cloud APM. IBM Cognos Viewer es el visor de salida de informes predeterminado.

Informes de Agente de Supervisión de tiempo de respuesta

Para ver los informes **Uso y rendimiento de la aplicación** o **Comparar rendimiento de la aplicación en dos periodos de tiempo**, seleccione una aplicación que incluye los sistemas gestionados del Agente de Supervisión de tiempo de respuesta y seleccione **Acciones** > **Lanzar a informes**.

Para ver el informe **Todas mis aplicaciones** o **Comparar rendimiento de varias aplicaciones**, seleccione **Todas mis aplicaciones**, y seleccione **Acciones** > **Lanzar a informes**.

Informes de Agente de WebSphere Applications

Para ver cualquier informe del Agente de WebSphere Applications, seleccione una aplicación que incluya sistemas gestionados de Agente de WebSphere Applications y seleccione **Acciones** > **Lanzar a informes**.

Agente de Synthetic Playback

Para ver cualquier informe del Agente de Synthetic Playback, seleccione una aplicación que incluya transacciones sintéticas y seleccione **Acciones** > **Lanzar a informes**.

Nota: Si la opción **Lanzar para informes** no se encuentra en el menú **Acciones**, compruebe que los informes de Cloud APM se hayan instalado correctamente.

Si desea información sobre los navegadores soportados para visualizar informes de Agente de Synthetic Playback, Agente de Supervisión de tiempo de respuesta y Agente de WebSphere Applications, consulte los Informes de compatibilidad de producto paraCognos 10.2.1.7.

Informes de Agente de Supervisión de tiempo de respuesta

Hay disponibles informes históricos de los datos recopilados por el Agente de Supervisión de tiempo de respuesta. Los informes de Agente de Supervisión de tiempo de respuesta no están disponibles en Cloud APM, Base. Sólo están disponibles en Cloud APM, Advanced.

Hay dos tipos de informes disponibles de los datos recopilados por el Agente de Supervisión de tiempo de respuesta: activos y simples.

Informes activos
Los informes activos se ven en un navegador en formato MHTML. Internet Explorer soporta MHTML de forma predeterminada. Para otros navegadores, se puede instalar un plug-in de soporte MHTML. Los informes activos se conocen también como informes interactivos fuera de línea.

Informes simples
Los informes simples se ven en IBM Cognos Viewer. IBM Cognos Viewer es el visor de salida de informes predeterminado.

Hay disponibles los siguientes informes históricos predefinidos de los datos recopilados por el Agente de Supervisión de tiempo de respuesta:

Tabla 254. Informes históricos predefinidos

Informe	**Tipo**
Todas mis aplicaciones	Activo
Uso y rendimiento de la aplicación	Activo
Comparar rendimiento de la aplicación en dos periodos de tiempo	Simple
Comparar rendimiento de varias aplicaciones	Simple

Los datos de los informes se almacenan en la base de datos Db2 DATAMART. Los informes muestran datos resumidos diariamente, semanalmente y mensualmente que se conservan durante 26 semanas, 12

meses y 3 años, respectivamente. Cloud APM no proporciona scripts ni instrucciones para cambiar estos periodos de retención.

Para obtener más información sobre la correlación entre el Agente de Supervisión de tiempo de respuesta y los informes de Performance Management, consulte Correlación de atributos del agente Supervisión de tiempo de respuesta.

Informe Todas mis aplicaciones
Utilice el informe Todas mis aplicaciones para ver información sobre los dispositivos de usuarios, el volumen de datos, el tiempo de respuesta y los recuentos de errores.

En este informe puede ver información de todas las aplicaciones. Especifique el periodo de tiempo del informe como **Último día** (predeterminado), **Última semana** o **Último mes**. Puede ver la información siguiente por periodo de tiempo seleccionado por aplicación:

- Diagrama de columnas apiladas de recuento de transacciones
- Diagrama de columnas de volumen de datos de transacción
- Diagrama de columnas de tiempo de respuesta de transacción promedio
- Diagrama de columnas apiladas de recuentos de error

Informe de uso y rendimiento de la aplicación
Utilice este informe para ver el rendimiento, la disponibilidad y la información de dispositivos de usuario para aplicaciones individuales.

En la ventana **Seleccionar una aplicación** seleccione una aplicación. Pulse **Siguiente**. En **Seleccionar transacciones clave para la aplicación**, seleccione la transacción o las transacciones por las que desea filtrar el informe. Pulse **Aceptar**. Este informe tiene tres pestañas: Rendimiento, Disponibilidad y Dispositivos. El intervalo de tiempo predeterminado es semana.

En la pestaña Rendimiento, vea la información siguiente por el intervalo de tiempo seleccionado para la aplicación que está viendo actualmente en el Panel de instrumentos de rendimiento de aplicaciones:

- Diagrama de líneas de tiempo de respuesta promedio por transacciones (clave)
- Diagrama de líneas de tiempo de respuesta de transacción promedio por éxito, error de servidor y error de cliente
- Diagrama de barras y de líneas de volumen de datos de transacción; las barras muestran el volumen de datos de transacción y la línea muestra el promedio de volumen de datos de transacción
- Diagrama de barras y de líneas de recuento de transacciones, las barras muestran el recuento de transacciones y la línea muestra valores polinómicos y promedio de movimiento

En la pestaña Disponibilidad, vea la información siguiente por el intervalo de tiempo seleccionado para la aplicación que está viendo actualmente en el Panel de instrumentos de rendimiento de aplicaciones:

- Diagrama de barras apiladas del porcentaje de transacciones satisfactorias frente a fallidas; los fallos se desglosan en errores de servidor y errores de cliente
- Diagrama de barras apiladas del porcentaje de recuentos de transacciones satisfactorias frente a fallidas por tipos de dispositivos; los fallos se desglosan en errores de servidor y errores de cliente
- Diagrama circular de los códigos de error que se producen con mayor frecuencia

En la pestaña Dispositivos, vea la información siguiente por el intervalo de tiempo seleccionado para la aplicación que está viendo actualmente en el Panel de instrumentos de rendimiento de aplicaciones:

- Diagrama de barras de transacciones por tipo de dispositivo
- Diagrama de barras de transacciones por sistema operativo de dispositivo
- Diagrama de barras de transacciones por navegador de dispositivo
- Tabla que muestra el rendimiento de transacciones por dimensiones; puede filtrar esta tabla en función del tipo de dispositivo, el sistema operativo de dispositivo, la marca de dispositivo y el navegador de dispositivos

Informe Comparar rendimiento de la aplicación en dos periodos de tiempo
Utilice este informe para examinar el rendimiento de la aplicación para una aplicación seleccionada.

En la ventana **Seleccionar aplicación y frecuencia**, especifique una aplicación y una frecuencia de tiempo (semanal, diaria, mensual). En la ventana **Seleccionar periodos de tiempo** elija periodos de tiempo adecuados al intervalo de tiempo y pulse **Aceptar**.

El informe visualiza los diagramas siguientes para la aplicación seleccionada, para los periodos de tiempo seleccionados por el intervalo de tiempo seleccionado:

- Diagrama de líneas de recuento de transacciones para tipo de dispositivo
- Diagrama de líneas de volumen de transacciones
- Diagrama de líneas de tiempo de respuesta de transacción promedio
- Diagrama de líneas de recuentos de errores

Informe Comparación del rendimiento de varias aplicaciones
Utilice este informe para comparar el rendimiento de varias aplicaciones durante el mismo periodo de tiempo.

En **Seleccione aplicaciones y frecuencia**, especifique una aplicación y una frecuencia (semanal, diaria, mensual). Pulse **Siguiente**. Elija un periodo de tiempo adecuado para el intervalo de tiempo.

El informe visualiza los diagramas siguientes para la aplicación seleccionada, para el periodo de tiempo seleccionado por la frecuencia seleccionada:

- Diagrama de líneas de recuento de transacciones
- Diagrama de líneas de volumen de datos de transacción
- Diagrama de líneas de tiempo de respuesta de transacción promedio
- Diagrama de líneas de recuentos de errores

Correlación de atributos de Agente de Supervisión de tiempo de respuesta
Algunos informes de Cloud APM se basan en datos recopilados por el Agente de Supervisión de tiempo de respuesta. Los datos de estos informes se correlacionan con atributos del Agente de Supervisión de tiempo de respuesta.

En la tabla siguiente se proporciona la correlación de elementos de datos en informes del Agente de Supervisión de tiempo de respuesta con los atributos del agente:

Tabla 255. Correlación de atributos del Agente de Supervisión de tiempo de respuesta

Elemento de datos de informe	Descripción	Nombre de atributo ODI	Columna de archivo ODI
Nombre de aplicación	El nombre de la aplicación supervisada informada a la Consola de Cloud APM	Nombre de aplicación	T5TXCS.APPLICATIN
Recuento de transacciones	El número total de secuencias de solicitud y respuesta observadas por el agente de supervisión durante el intervalo agregado actual.	Número total de solicitudes	T5TXINS.TOTREQ

Tabla 255. Correlación de atributos del Agente de Supervisión de tiempo de respuesta (continuación)

Elemento de datos de informe	Descripción	Nombre de atributo ODI	Columna de archivo ODI
Errores de cliente	El número de solicitudes HTTP cuyo código de estado está entre 400 y 499.	Errores de cliente	T5TXCS.NUM4XX
Errores de servidor	El número de solicitudes HTTP cuyo código de estado está entre 500 y 599.	Errores de servidor	T5TXCS.NUM5XX
Nombre de transacción	El nombre de la transacción notificado a Application Management Console.	Nombre de transacción	T5TXCS.TRANSACTN
Estado de transacción	El código de respuesta que está asociado a la transacción	Código de estado	T5TXCS.STATUSCODE
Kilobytes de respuesta de código	El número total de kilobytes en cada respuesta de la solicitud durante el intervalo de datos.	Bytes de respuesta	T5TXCS.REPLYBYT
Kilobytes de solicitud	El número total de kilobytes de la solicitud durante el intervalo de datos.	kBytes de solicitud	T5TXCS.REQBYTES
Número total de Kilobytes	El número total de kilobytes transferidos para toda la solicitud durante el periodo de tiempo.	Bytes totales	T5TXCS.TOTBYTES
Recuento total de objetos	El número total de objetos incluidos en una página web para el periodo de tiempo	Recuento total de objetos	T5TXCS.OBJCNT
Tamaño total de objeto	El tamaño total de todos los objetos incluidos en la página web para el periodo de tiempo.	Tamaño total de objeto	T5TXCS.OBJSIZE
Tiempo de respuesta (segundos)	El número total de segundos necesarios para que se complete la transacción de servidor global.	Tiempo de respuesta	T5TXCS.RESPTIME

Tabla 255. Correlación de atributos del Agente de Supervisión de tiempo de respuesta (continuación)			
Elemento de datos de informe	**Descripción**	**Nombre de atributo ODI**	**Columna de archivo ODI**
Tiempo de representación	El tiempo transcurrido, en segundos, para representar totalmente la página web en el navegador web utilizando códigos JavaScript incluidos.	Tiempo de representación	T5TXCS.RENDERTIME
Tiempo de cliente	El tiempo promedio transcurrido, en segundos, mientras la transacción está en ejecución en el cliente durante el intervalo de supervisión actual.	Tiempo de cliente promedio	T5TXCS.CLIENTTIME
Tiempo de carga	El tiempo promedio transcurrido, en segundos, desde el momento en que el usuario solicita una descarga hasta que se lleva a cabo la descarga del objeto web.	Tiempo de carga promedio	T5TXCS.LOADTIME
Navegador	Una descripción del navegador web en el que se muestra la página web.	Descripción de navegador	T5TXCS.BROWSEDESC
Servidor	Nombre o dirección IP del servidor para la transacción TCP.	Descripción de servidor	T5TXCS.SERVERDESC
Nombre de host de URL	El nombre de host TCP/IP del URL.	Nombre de host de URL	T5TXCS.URLHOST
Método de URL	El método utilizado para realizar solicitudes HTTP (GET, POST, HEAD, PUT, OPTIONS, DELETE, TRACE o CONNECT).	Método	T5TXCS.METHOD
Detalles de URL	Vía de acceso de URL del archivo en el servidor donde reside la página web.	Vía de acceso de URL	T5TXCS.URLPATH

Para obtener más información acerca del Agente de Supervisión de tiempo de respuesta, consulte Transaction Monitoring Reference.

Generación de informes de Agente de Synthetic Playback

Ejecute los informes para las aplicaciones asociadas a las transacciones sintéticas.

Acerca de esta tarea

Seleccione una aplicación y una transacción sintética asociada en el Panel de instrumentos del rendimiento de aplicaciones y luego genere los informes basándose en la selección. Los datos de los informes se almacenan en la base de datos Db2 DATAMART. Los informes muestran datos resumidos cada hora, semanalmente y mensualmente que se conservan durante 371 días, 53 semanas y 12 meses, respectivamente. Cloud APM no proporciona scripts ni instrucciones para cambiar estos periodos de retención.

Están disponibles cinco informes de múltiples páginas:

Global de transacciones

Este informe de dos páginas muestra los tiempos de respuesta y las tasas de disponibilidad de la transacción sintética seleccionada durante un rango de fechas definido.

La página uno muestra los datos siguientes:

- Un gráfico de líneas de los tiempos de respuesta de las transacciones sintéticas seleccionadas en intervalos establecidos durante un rango de fechas definido
- Una tabla de los tiempos medios de respuesta en segundos de cada transacción sintética en el intervalo de fechas definido

La página dos muestra los datos siguientes:

- Un gráfico de líneas de las tasas de disponibilidad de las transacciones sintéticas seleccionadas a intervalos establecidos durante un rango de fechas definido
- Una tabla de la tasa media de disponibilidad de cada transacción sintética en el intervalo de fechas definido

Puede acceder a dos informes adicionales desde el informe **Global de transacciones**, **Análisis puntual por transacciones** y **Métricas HTTP por transacciones**.

Análisis puntual por transacciones muestra métricas HTTP de la transacción sintética seleccionada a intervalos establecidos durante un rango de fechas definido. El informe incluye los siguientes elementos:

- Un gráfico de columnas de las métricas HTTP de la transacción sintética seleccionada a intervalos establecidos durante un rango de fechas establecido
- Una tabla de las métricas HTTP en milisegundos de la transacción sintética seleccionada durante el rango de fechas definido

Métricas HTTP por transacción muestra métricas HTTP de la transacción sintética seleccionada a intervalos establecidos durante un rango de fechas definido. El informe incluye los siguientes elementos:

- Un gráfico de columnas de las métricas HTTP de la transacción sintética seleccionada a intervalos establecidos durante un rango de fechas establecido
- Una tabla de las métricas HTTP en milisegundos de la transacción sintética seleccionada durante el rango de fechas definido

Detalle de transacción por ubicaciones

Este informe de dos páginas muestra los tiempos de respuesta y las tasas de disponibilidad por ubicación de las transacciones y subtransacciones sintéticas seleccionadas durante un rango de fechas definido.

La página uno muestra los datos siguientes:

- Un gráfico de líneas de los tiempos de respuesta por ubicación de las transacciones sintéticas seleccionadas y las subtransacciones a intervalos establecidos durante un rango de fechas definido

- Las tablas de los tiempos medios de respuesta en segundos de todas las subtransacciones sintéticas en un intervalo de fechas definido en cada ubicación

La página dos muestra los datos siguientes:

- Un gráfico de líneas de las tasas de disponibilidad por ubicación de las transacciones sintéticas seleccionadas y las subtransacciones a intervalos establecidos durante un rango de fechas definido
- Las tablas de las tasas medias de disponibilidad de todas las subtransacciones sintéticas durante un intervalo de fechas definido en cada ubicación

Puede acceder cuatro informes adicionales desde el informe **Detalle de transacción por ubicaciones**, **Análisis puntual por ubicaciones de transacción**, **Métricas HTTP por ubicaciones de transacción**, **Análisis puntual por ubicaciones de subtransacción** y **Métricas HTTP por ubicaciones de subtransacción**.

Análisis puntual por ubicaciones de transacción muestra métricas HTTP de la transacción sintética por ubicaciones a intervalos establecidos durante un rango de fechas definido. El informe incluye los siguientes elementos:

- Un gráfico de columnas de las métricas HTTP de la transacción sintética seleccionada por ubicaciones a intervalos establecidos durante el rango de fechas establecido
- Una tabla de las métricas HTTP en milisegundos de la transacción sintética seleccionada por ubicaciones durante el rango de fechas definido

Métricas HTTP por ubicaciones de transacción muestra métricas HTTP de la transacción sintética por ubicaciones a intervalos establecidos durante un rango de fechas definido. El informe incluye los siguientes elementos:

- Un gráfico de columnas de las métricas HTTP de la transacción sintética seleccionada por ubicaciones a intervalos establecidos durante el rango de fechas establecido
- Una tabla de las métricas HTTP en milisegundos de la transacción sintética seleccionada por ubicaciones durante el rango de fechas definido

Análisis puntual por ubicaciones de subtransacción muestra métricas HTTP de una subtransacción por ubicaciones a intervalos establecidos durante un rango de fechas definido. El informe incluye los siguientes elementos:

- Un gráfico de columnas de las métricas HTTP de la subtransacción seleccionada por ubicaciones a intervalos establecidos durante el rango de fechas establecido
- Una tabla de las métricas HTTP en milisegundos de la subtransacción seleccionada por ubicaciones durante el rango de fechas definido

Métricas HTTP por ubicaciones de subtransacción muestra métricas HTTP de una subtransacción sintética por ubicaciones a intervalos establecidos durante un rango de fechas definido. El informe incluye los siguientes elementos:

- Un gráfico de columnas de las métricas HTTP de la subtransacción seleccionada por ubicaciones a intervalos establecidos durante el rango de fechas establecido
- Una tabla de las métricas HTTP en milisegundos de la subtransacción seleccionada por ubicaciones durante el rango de fechas definido

Detalle de transacción por subtransacciones

Este informe de dos páginas muestra los tiempos de respuesta y las tasas de disponibilidad de subtransacciones sintéticas a intervalos definidos durante un rango de fechas definido.

La página uno muestra los datos siguientes:

- Un gráfico de líneas de los tiempos de respuesta de las subtransacciones sintéticas seleccionadas a intervalos establecidos durante un rango de fechas definido
- Una tabla de los tiempos medios de respuesta en segundos de cada subtransacción sintética en el intervalo de fechas definido

La página dos muestra los datos siguientes:

- Un gráfico de líneas de las tasas de disponibilidad de las subtransacciones sintéticas seleccionadas a intervalos establecidos durante un rango de fechas definido
- Una tabla de las tasas de disponibilidad de cada subtransacción sintética en el intervalo de fechas definido

Puede acceder a dos informes adicionales desde el informe **Detalle de transacción por subtransacciones**, **Análisis puntual por subtransacciones** y **Métricas HTTP por subtransacciones**.

Análisis puntual por ubicaciones de subtransacción muestra métricas HTTP de una subtransacción por ubicaciones a intervalos establecidos durante un rango de fechas definido. El informe incluye los siguientes elementos:

- Un gráfico de columnas de las métricas HTTP de la subtransacción seleccionada a intervalos establecidos durante un rango de fechas establecido
- Una tabla de las métricas HTTP en milisegundos de la subtransacción seleccionada durante el rango de fechas definido

Métricas HTTP por ubicaciones de subtransacción muestra métricas HTTP de una subtransacción sintética por ubicaciones a intervalos establecidos durante un rango de fechas definido. El informe incluye los siguientes elementos:

- Un gráfico de columnas de las métricas HTTP de la subtransacción seleccionada a intervalos establecidos durante un rango de fechas establecido
- Una tabla de las métricas HTTP en milisegundos de la subtransacción seleccionada durante el rango de fechas definido

Tendencia de transacciones

Este informe de cuatro páginas muestra un análisis de tendencias de tiempos de respuesta, tasas de disponibilidad y métricas HTTP durante la semana anterior y durante las cinco semanas anteriores.

La página uno muestra datos de tendencia sobre los tiempos de respuesta y las tasas de disponibilidad de una transacción sintética:

- Un gráfico de líneas combinado de los tiempos de respuesta promedio de una transacción sintética seleccionada durante la semana anterior y durante las 5 semanas anteriores
- Un gráfico de líneas combinado de la tasa de disponibilidad de una transacción sintética seleccionada que compara la tasa de disponibilidad durante la semana anterior con la tasa de disponibilidad de línea base durante las 5 semanas anteriores
- Una tabla del tiempo de respuesta promedio y la tasa de disponibilidad de una transacción sintética durante la semana anterior y durante el intervalo de fechas de 5 semanas anteriores
- Un gráfico de líneas combinado de los tiempos de respuesta promedio de una transacción sintética seleccionada durante la semana anterior y durante las 5 semanas anteriores, por ubicación
- Un gráfico de líneas combinado de la tasa de disponibilidad de una transacción sintética seleccionada que compara la tasa de disponibilidad durante la semana anterior con la tasa de disponibilidad de línea base durante las 5 semanas anteriores, por ubicación
- Una tabla de los tiempos de respuesta promedio y tasas de disponibilidad de una transacción sintética seleccionada durante la semana anterior y durante las 5 semanas anteriores, por ubicación
- Un gráfico de líneas combinado de los tiempos de respuesta promedio de las subtransacciones de una transacción sintética seleccionada durante la semana anterior y durante las 5 semanas anteriores
- Un gráfico de líneas combinado de las tasas de disponibilidad promedio de las subtransacciones de una transacción sintética seleccionada que compara la tasa de disponibilidad durante la semana anterior con la tasa de disponibilidad de línea base durante las 5 semanas anteriores
- Una tabla de los tiempos de respuesta promedio y las tasas de disponibilidad de las subtransacciones de una transacción sintética seleccionada durante la semana anterior y durante las 5 semanas anteriores

La página dos muestra los datos de tendencia de las métricas HTTP de una transacción sintética:

- Un gráfico de líneas combinado de los tiempos de bloqueo promedio de una transacción sintética seleccionada durante la semana anterior y durante las últimas cinco semanas
- Un gráfico de líneas combinado de los tiempos de DNS promedio de una transacción sintética seleccionada durante la semana anterior y durante las últimas cinco semanas
- Un gráfico de líneas combinado de los tiempos de SSL promedio de una transacción sintética seleccionada durante la semana anterior y durante las últimas cinco semanas
- Un gráfico de líneas combinado de los tiempos de conexión promedio de una transacción sintética seleccionada durante la semana anterior y durante las últimas cinco semanas
- Un gráfico de líneas combinado de los tiempos de envío promedio de una transacción sintética seleccionada durante la semana anterior y durante las últimas cinco semanas
- Un gráfico de líneas combinado de los tiempos de recepción promedio de una transacción sintética seleccionada durante la semana anterior y durante las últimas cinco semanas
- Un gráfico de líneas combinado de los tiempos de representación promedio de una transacción sintética seleccionada durante la semana anterior y durante las últimas cinco semanas
- Una tabla de métricas HTTP promedio de una transacción sintética durante la semana anterior y durante las últimas cinco semanas

La página tres muestra datos de tendencia sobre métricas HTTP en milisegundos de una transacción sintética por ubicación. Los gráficos y la tabla comparan los promedios de métricas HTTP durante la semana anterior con el promedio de métricas de línea base durante las últimas 5 semanas:

- Siete diagramas de líneas combinados que comparan distintas métricas HTTP promedio de una transacción sintética seleccionada durante la semana anterior con la métrica de línea base durante las últimas 5 semanas por ubicación
- Una tabla de métricas HTTP promedio de una transacción sintética seleccionada durante la semana anterior y durante las últimas cinco semanas por ubicación

La página cuatro muestra los datos de tendencia de las métricas HTTP en milisegundos de subtransacciones. Los gráficos y la tabla comparan los promedios de métricas HTTP durante la semana anterior con el promedio de métricas de línea base durante las últimas 5 semanas:

- Siete diagramas de líneas combinados que comparan valores promedio de distintas métricas HTTP de una transacción sintética seleccionada durante la semana anterior con la métrica de línea base durante las últimas 5 semanas por subtransacción
- Una tabla de valores promedio de métricas HTTP de una transacción sintética seleccionada durante la semana anterior y durante las últimas cinco semanas por subtransacción

Tendencia de subtransacciones

Este informe de dos páginas muestra un análisis de tendencias de los tiempos de respuesta, las relaciones de disponibilidad y las métricas HTTP de subtransacciones durante la última semana y durante las últimas cinco semanas.

La página uno muestra los datos de tendencia sobre los tiempos de respuesta y las relaciones de disponibilidad de subtransacciones durante el domingo anterior, la semana anterior y las últimas cinco semanas:

- Una tabla que compara los tiempos de respuesta y las tasas de disponibilidad de subtransacciones desde el domingo anterior, la semana anterior y las últimas cinco semanas
- Un gráfico de líneas combinado que compara los tiempos de respuestas promedio de subtransacciones durante la semana anterior con el tiempo de respuesta de línea base durante las últimas cinco semanas
- Un gráfico de líneas combinado que compara la tasa de disponibilidad promedio de subtransacciones durante la semana anterior con la relación de disponibilidad de línea base durante las últimas cinco semanas
- Una tabla de tiempos de respuesta y tasas de disponibilidad promedio de subtransacciones durante la semana anterior.

- Una tabla de tiempos de respuesta y tasas de disponibilidad promedio de subtransacciones durante las cinco semanas anteriores.

La página dos muestra los datos de tendencia de las métricas HTTP en milisegundos de subtransacciones. Los gráficos y las tablas comparan los promedios de métricas HTTP de subtransacciones durante la semana anterior con los promedios de métricas de línea base durante las últimas cinco semanas:

- Siete tablas de valores promedio de métricas HTTP de la transacción seleccionada para el domingo anterior, la semana anterior y durante las últimas cinco semanas por subtransacciones
- Siete diagramas de líneas combinados que comparan distintas métricas HTTP promedio en milisegundos de la transacción seleccionada durante la semana anterior con la relación de disponibilidad de línea base durante las últimas 5 semanas por subtransacciones
- Una tabla de valores promedio de métricas HTTP de subtransacciones durante la semana anterior.
- Una tabla de valores promedio de métricas HTTP de subtransacciones durante las últimas cinco semanas.

Procedimiento

Para generar informes, lleve a cabo los pasos siguientes:

1. Pulse el icono **Rendimiento** y seleccione **Application Performance Dashboard**. Para elegir una aplicación, expanda **Todas mis aplicaciones** y seleccione una aplicación. Para mostrar todas las transacciones sintéticas asociadas a la aplicación seleccionada, pulse **Grupos** > **Transacciones** > **Transacciones sintéticas**.
2. Seleccione una transacción sintética de la tabla de lista de transacciones. Para ejecutar un informe, pulse **Acciones** > **Lanzar a informes** y seleccione uno de los informes siguientes:
   - **Global de transacciones**
   - **Detalle de transacción por ubicaciones**
   - **Detalle de transacción por subtransacciones**
   - **Tendencia de transacciones**
   - **Tendencia de subtransacciones**

   Se abrirá una página de configuración en una nueva pestaña del navegador web.
3. Para establecer el intervalo de fechas del informe, seleccione un intervalo de fechas predefinido o especifique un intervalo de fechas personalizado.
4. Para establecer el intervalo de tiempo del informe, seleccione un intervalo de **Tipo de temporización**. Establezca su informe para mostrar datos de las transacciones sintéticas y subtransacciones a intervalos **Cada hora** , **Diario** o **Semanal**, en el intervalo de fechas definido. Para generar el informe, pulse **Finalizar**.
5. Para ver informes sobre métricas HTTP de transacciones, subtransacciones o ubicaciones, debe seleccionar una transacción, subtransacción o ubicación en el informe **Global de transacciones**, **Detalle de transacción por ubicaciones** o **Detalle de transacción por subtransacciones**.
   - Para ver **Análisis puntual por transacciones**, pulse el botón derecho del ratón en un nombre de transacción en el informe de **Global de transacciones** y seleccione **Ir a** > **Análisis de métricas Http por tiempo**.
   - Para ver **Métricas HTTP por transacciones**, pulse el botón derecho del ratón en un nombre de transacción en el informe **Global de transacciones** y seleccione **Ir a** > **Agregación de métricas Http**.
   - Para ver **Análisis puntual por ubicaciones de transacción**, pulse el botón derecho del ratón en un nombre de transacción en el informe **Detalle de transacción por ubicaciones** y seleccione **Ir a** > **Análisis de métricas Http por tiempo**.
   - Para ver **Métricas HTTP por ubicaciones de transacción**, pulse el botón derecho del ratón en un nombre de transacción en el informe **Detalle de transacción por ubicaciones** y seleccione **Ir a** > **Agregación de métricas Http**.

- Para ver **Análisis puntual por ubicaciones de subtransacción**, pulse el botón derecho del ratón en un nombre de subtransacción en el informe **Detalle de transacción por ubicaciones** y seleccione **Ir a** > **Análisis de métricas Http por tiempo**.
- Para ver **Métricas HTTP por ubicaciones de subtransacción**, pulse el botón derecho del ratón en un nombre de subtransacción en el informe **Detalle de transacción por ubicaciones** y seleccione **Ir a** > **Agregación de métricas Http**.
- Para ver **Análisis puntual por subtransacciones**, pulse el botón derecho del ratón en un nombre de subtransacción en el informe de **Tendencia de subtransacciones** y seleccione **Ir a** > **Análisis de métricas Http por tiempo**.
- Para ver **Métricas HTTP por subtransacciones**, pulse el botón derecho del ratón en un nombre de subtransacción en el informe **Tendencia de subtransacciones** y seleccione **Ir a** > **Agregación de métricas Http**.

Informes de Agente de WebSphere Applications

Hay disponibles informes predefinidos de los datos recopilados por el Agente de WebSphere Applications.

Los datos de los informes se almacenan en la base de datos Db2 WAREHOUS. Los informes muestran datos cada hora, semanalmente y mensualmente que se conservan durante 1 mes, 3 meses, 1 año, respectivamente. Cloud APM no proporciona scripts ni instrucciones para cambiar estos periodos de retención. Hay disponibles los siguientes informes de los datos recopilados por el Agente de WebSphere Applications:

Rendimiento de solicitudes de la aplicación

Descripción

Este informe analiza cómo se ejecutan las aplicaciones en un nivel de agregado a través de un servidor de aplicaciones. El diagrama circular muestra las solicitudes de nivel de agregado de las aplicaciones. El diagrama de barras muestra el tiempo medio de respuesta de las aplicaciones a un nivel de agregado. Los dos diagramas cronológicos muestran el tiempo de respuesta medio y la tendencia de recuento total de solicitudes de todas las aplicaciones. Para descender a mayor nivel de detalle en las solicitudes individuales de una aplicación, pulse una porción circular o una barra.

Parámetros

Intervalo de fechas: seleccione uno de los periodos del informe predefinidos o seleccione las horas de inicio y finalización exactas del calendario.

Parámetros necesarios: tipo de resumen y tipo de servidor de aplicaciones

Tablas utilizadas

Request_Analysis_*V

Agrupaciones de conexiones de BD

Descripción

Este informe analiza las agrupaciones de conexiones de base de datos en un servidor de aplicaciones. En la tabla se muestran las estadísticas clave de todas las agrupaciones de conexiones en un nivel de agregado. Cuando selecciona un origen de datos específico, dos diagramas de tendencias muestran la tendencia de las estadísticas clave.

Parámetros

Intervalo de fechas: seleccione uno de los periodos del informe predefinidos o seleccione las horas de inicio y finalización exactas del calendario.

Parámetros necesarios: tipo de resumen y nombre de servidor de aplicaciones

Tablas utilizadas

DB_Connection_Pools_*V

Rendimiento de EJB

Descripción

Este informe analiza cómo se ejecutan los EJB desplegados en el servidor de aplicaciones. El diagrama circular muestra el recuento de métodos de nivel de agregado de EJB. El diagrama de barras muestra el tiempo de respuesta de método promedio en los EJB a un nivel de agregado. Los dos diagramas cronológicos muestran la tendencia de recuento de invocaciones del método y la tendencia de tiempo de respuesta medio de método de todos los EJB. Las líneas de tendencia se pueden filtrar por EJB pulsando una fila de la lista.

Parámetros

Intervalo de fechas: seleccione uno de los periodos del informe predefinidos o seleccione las horas de inicio y finalización exactas del calendario.

Parámetros necesarios: tipo de resumen y nombre de servidor de aplicaciones

Tablas utilizadas

Enterprise_Java_Beans_*V

Uso de RB de servidor de aplicaciones

Descripción

Este informe analiza la recogida de basura. Utilice este informe para determinar si la recogida de basura está creando problemas o si el almacenamiento dinámico no está dimensionado correctamente. El primer gráfico muestra el porcentaje promedio de almacenamiento dinámico que se utiliza y el porcentaje promedio en tiempo real de recogida de basura a lo largo del tiempo. El segundo diagrama muestra el promedio de porcentaje en tiempo real de ejecuciones de recogida de basura y el promedio de frecuencia recogida de basura.

Parámetros

Intervalo de fechas: seleccione uno de los periodos del informe predefinidos o seleccione las horas de inicio y finalización exactas del calendario.

Parámetros necesarios: tipo de resumen, tipo de servidor de aplicaciones

Tablas utilizadas

Garbage_Collection_Analysis_*V

Uso de JVM de servidor de aplicaciones

Descripción

Este informe analiza cómo se ejecuta la máquina virtual Java de un servidor de aplicaciones. El diagrama de barras apiladas muestra cómo se utiliza la memoria de máquina virtual Java y cómo se libera. El diagrama de líneas duales muestra el consumo de CPU de la JVM frente al uso de la memoria de la JVM.

Parámetros

Intervalo de fechas: seleccione uno de los periodos del informe predefinidos o seleccione las horas de inicio y finalización exactas del calendario.

Parámetros necesarios: tipo de resumen, tipo de servidor de aplicaciones

Tablas utilizadas

Application_Server_*V

Agrupaciones de hebras

Descripción

Este informe analiza las agrupaciones de hebras en un servidor de aplicaciones. En la tabla se muestran las estadísticas clave de todas las agrupaciones de hebras en un nivel de agregado. Una vez seleccionada una agrupación de hebras de la lista, el diagrama de tendencias muestra la tendencia de las estadísticas clave de la agrupación de hebras seleccionada. Si no se selecciona ninguna agrupación de hebras, las tendencias muestran el resumen de todas las agrupaciones de hebras.

Parámetros

Intervalo de fechas: seleccione uno de los periodos de informe predefinidos o seleccione las horas de inicio y finalización exactas del calendario

Parámetros necesarios: tipo de resumen, tipo de servidor de aplicaciones

Tablas utilizadas

Thread_Pools_*V

Rendimiento de aplicaciones web

Descripción

Este informe analiza cómo se ejecutan las aplicaciones en el contenedor web de un servidor de aplicaciones (datos PMI). Los diagramas circulares muestran las solicitudes de nivel de agregado de las aplicaciones. El diagrama de barras muestra el tiempo medio de respuesta de las aplicaciones a un nivel de agregado. Los dos diagramas cronológicos muestran el tiempo de respuesta medio y la tendencia de recuento total de solicitudes de todas las aplicaciones. Pulse una sección circular o una barra o una línea para descender a mayor nivel de detalle en el servlet/jsps individual de esa aplicación.

Parámetros

Intervalo de fechas: seleccione uno de los periodos del informe predefinidos o seleccione las horas de inicio y finalización exactas del calendario.

Parámetros necesarios: tipo de resumen, tipo de servidor de aplicaciones

Tablas utilizadas

Thread_Pools_*V

Rendimiento de solicitudes de la aplicación para clústeres

Descripción

Este informe analiza cómo se ejecutan los servidores en un clúster. La primera gráfica muestra el número de solicitudes que se han completado por cada uno de los miembros del clúster durante el intervalo de tiempo seleccionado. El segundo diagrama proporciona información sobre el promedio de tendencia de tiempo de respuesta para cada uno de los miembros de clúster. Hay una línea aparte en este diagrama para cada servidor del clúster. Pulse una línea para descender a mayor nivel de detalle en los datos de servidor individual. Se abre el informe Rendimiento de solicitudes de la aplicación para este servidor

Parámetros

Intervalo de fechas: seleccione uno de los periodos del informe predefinidos o seleccione las horas de inicio y finalización exactas del calendario.

Parámetros necesarios: tipo de resumen y nombre de clúster

Tablas utilizadas

Request_Analysis_*V

Uso de JVM y RB para clústeres

Descripción

Este informe analiza las tendencias de uso de máquina virtual Java y de recogida de basura por parte de cada uno de los miembros de clúster. El primer diagrama muestra el porcentaje medio en tiempo real de ejecuciones de recogida de basura. El segundo diagrama muestra el porcentaje medio de almacenamiento dinámico utilizado. Los últimos diagramas muestran el uso de CPU y de memoria de JVM. Todos estos diagramas muestran los datos de cada miembro de clúster como una línea aparte.

Parámetros

Intervalo de fechas: seleccione uno de los periodos del informe predefinidos o seleccione las horas de inicio y finalización exactas del calendario.

Parámetros necesarios: tipo de resumen y nombre de clúster

Tablas utilizadas

Garbage_Collection_Analysis_*V, Application_server_*V

Principales aplicaciones con tiempos de respuesta más lentos entre servidores

Descripción

Este informe analiza cómo se ejecutan las aplicaciones en un nivel de agregado a través de todos los servidores de aplicaciones. Un diagrama de barras muestra el tiempo medio de respuesta de las aplicaciones a un nivel de agregado.

Parámetros

Intervalo de fechas: seleccione uno de los periodos del informe predefinidos o seleccione las horas de inicio y finalización exactas del calendario.

Parámetros necesarios: tipo de resumen, número de aplicaciones

Capítulo 11. Actualización

Actualice los agentes y recopiladores de datos para obtener las características y la funcionalidad más recientes disponibles en el release actual.

Actualización de los agentes

De forma periódica, hay nuevos archivos de archivado que contienen agentes de supervisión actualizados disponibles para su descarga. Los archivos de archivado están disponibles enProductos y servicios en el sitio web de IBM Marketplace.

Antes de empezar

Para los agentes siguientes, se debe completar una tarea específica del agente antes de completar el procedimiento de actualización.

- Para los agentes en AIX, si realiza la ejecución como un usuario no root, debe borrar una de las bibliotecas de memoria antes de iniciar el procedimiento de instalación para actualizar el agente. Siga las instrucciones de “Agentes en AIX: Detención del agente y ejecución de slibclean antes de actualizar” en la página 1176.
- Para Agente de HMC Base en AIX, si actualiza el agente como usuario no root, primero debe detener Agente de HMC Base y limpiar de la memoria caché las bibliotecas dependientes. Siga las instrucciones que encontrará en “Agente de HMC Base en AIX: Detención del agente como usuario no root y ejecución de slibclean antes de actualizar” en la página 1177
- Para el Agente de Microsoft .NET, debe eliminar el recopilador de datos de las aplicaciones .NET antes de actualizar el agente. Siga las instrucciones de “Agente de Microsoft .NET: Eliminación del recopilador de datos .NET antes de actualizar” en la página 1179.
- Para el Agente de Node.js, debe eliminar los plug-in de recopilador de datos de las aplicaciones Node.js antes de actualizar el agente. Siga las instrucciones de “Agente de Node.js: Eliminación de los plug-in de recopilador de datos antes de actualizar” en la página 1177.
- Para el Agente de Ruby, debe eliminar el recopilador de datos de las aplicaciones Ruby antes de actualizar el agente. Siga las instrucciones de “Agente de Ruby: Eliminación de los plug-in de recopilador de datos antes de actualizar” en la página 1180.
- Para el Agente de HTTP Server, debe detener el servidor HTTP antes de actualizar el agente.
- Para el Agente de WebSphere MQ, si ha habilitado el rastreo de transacciones para el agente en el release anterior, debe detener la instancia del agente antes de actualizarlo.
- Para el Agente de SAP NetWeaver Java Stack, si está actualizando desde V8.1.3.2 a V8.1.4, detenga todas las instancias de SAP NetWeaver Java Stack que estén configuradas con el recopilador de datos antes de actualizar el agente.
- Para el Agente de Skype for Business Server, si está realizando una actualización desde una versión anterior a la 8.1.4.0.2, en el lado del agente, el nombre del agente cambia a Skype for Business Server. Además, tras la actualización de soporte mediante SDA, tiene que volver a iniciar el servicio APMUI para que refleje el nombre del nuevo agente (Skype for Business Server) en el lago del servidor de MIN o de lo contrario verá el nombre del agente anterior (MS Lync Server) en el panel de instrumentos del servidor de MIN.
- Para Agente de Tomcat, si desea actualizar la infraestructura principal de TEMA en Windows, debe detener tanto el agente como el servidor. Siga las instrucciones en Agente de Tomcat: Actualización de la infraestructura principal de TEMA en Windows

Acerca de esta tarea

Si hay una nueva versión del agente disponible, la ejecución del script de instalación actualiza automáticamente el agente. Si no se dispone de una versión más reciente del agente, aparece un mensaje que explica que el agente ya está instalado; no afecta al agente instalado.

Para instalar un agente actualizado, siga los procedimientos siguientes:

Procedimiento

- "Instalación de agentes en sistemas UNIX" en la página 126
- "Instalación de agentes en sistemas Linux" en la página 132
- "Instalación de agentes en sistemas Windows" en la página 141

Resultados

El agente se actualiza a la última versión. Si no está disponible una versión más reciente del agente de supervisión, aparece un mensaje que explica que el agente ya está instalado; no afecta al agente instalado.

Qué hacer a continuación

Después de una actualización de un agente Windows, debe reiniciar todos los agentes que el instalador de Windows no configura e inicia automáticamente. Ejecute el siguiente mandato para comprobar el estado del agente:

```
./nombre-agent.bat status
```

Utilice uno de los métodos siguientes para iniciar el agente:

- Pulse **Inicio** > **Todos los programas** > **Agentes de IBM Monitoring** > **IBM Performance Management**. Pulse el botón derecho del ratón en un agente y pulse **Iniciar**.
- Ejecute el mandato siguiente:

  ```
  ./nombre-agent.bat start
  ```

Para obtener más información sobre los mandatos de agente de supervisión, incluido el nombre que se va a utilizar, como comprobar el estado del agente, y más, consulte "Utilización de mandatos de agente" en la página 184. Si desea información sobre qué agentes se inician de forma automática y manual, consulte Capítulo 5, "Despliegue de agentes y recopiladores de datos", en la página 117

- Para el Agente de Hadoop, realice los pasos siguientes después de la actualización del agente basado en socket (8.1.2, Fixpack 2 o anterior) al agente basado en la API REST (8.1.3 o posterior):

  1. Para evitar la generación de registros innecesarios, elimine el código de 17 líneas de los archivos `hadoop-metrics2.properties` de todos los nodos Hadoop.
  2. Detenga los servicios de Hadoop.
  3. Suprima el archivo `Plugin.jar` que se ha copiado desde el instalador del agente desde todos los nodos del clúster de Hadoop.
  4. Inicie los servicios de Hadoop.

  Para obtener información sobre el código de 17 líneas y el archivo `Plugin.jar`, consulte Configuración de nodos Hadoop.
- Para el Agente de HMC Base, después de actualizar el agente de la versión 6.2.2.6 a 6.2.2.7, debe configurar el agente de nuevo y reiniciarlo. Para obtener instrucciones, consulte "Configuración de la supervisión de HMC Base" en la página 273.
- Para el Agente de HTTP Server, si actualiza el agente desde una versión anterior a 1.0.0.4 a la versión 1.0.0.4 o posterior, también debe actualizar el archivo `.conf`, utilizado por HTTP Server para sustituir el archivo de configuración de recopilador de datos anterior por el nuevo archivo generado. También

debe añadir la nueva instancia de agente a la consola. Para obtener instrucciones, consulte "Configuración de la supervisión de HTTP Server" en la página 278.

- Para el Agente de Microsoft .NET, después de actualizar el agente, configure el recopilador de datos. Para obtener instrucciones, consulte "Registro del recopilador de datos" en la página 542.

  Si ha instalado el agente en un directorio nuevo, debe cambiar la vía de acceso Bin del servicio Perfilador mediante el mandato de controlador de servicio (sc). Por ejemplo,

  ```
  sc \\localhost config DotNetProfilerService binPath=
  "${dir_instalación}\qe\bin\DotNetProfilerService.exe
  ```

  donde *dir_instalación* es el directorio de instalación nuevo.
- Para el Agente de Node.js, después de actualizar el agente, configure los recopiladores de datos de agente. Si desea más instrucciones, consulte "Configuración del Agente de Node.js" en la página 609.
- Para el Agente de OpenStack, para configurar el agente con mayor detalle para utilizar la API de identidad de OpenStack v3, reconfigure todas las instancias de agente y actualice el archivo de configuración del recopilador de datos del agente. Para obtener instrucciones, consulte "Agente de OpenStack: Reconfiguración de instancias de agente para utilizar la API de identidad de OpenStack v3" en la página 1180.
- Para el Agente de Ruby, después de actualizar el agente, configure el recopilador de datos. Si desea más instrucciones, consulte "Configuración del recopilador de datos de diagnóstico" en la página 747.
- Para el Agente de WebSphere Applications, después de actualizar el agente, migre el recopilador de datos ejecutando el mandato *dir_inicio_dc*`/bin/migrate.sh/bat` desde el directorio de instalación de la nueva versión del agente y reinicie la instancia del servidor de aplicaciones. Si desea más instrucciones, consulte "Agente de WebSphere Applications: Migración del recopilador de datos" en la página 1181.
- Linux Si desea actualizar una versión más antigua del agente que está instalada en el directorio `/opt/ibm/ccm/agent`, debe completar estos pasos en el sistema Linux:

  1. Si confirma que desea migrar la configuración de agente del directorio de instalación antiguo `/opt/ibm/ccm/agent` al directorio de instalación nuevo, por ejemplo `/opt/ibm/apm/agent`, debe iniciar el agente en la ubicación de instalación nueva.

     Restricción: La versión más antigua del agente se detiene automáticamente en la ubicación de instalación antigua pero no se inicia automáticamente en la ubicación de instalación nueva.
  2. Tras verificar que el agente trabaja en el nuevo directorio de instalación, debe desinstalar la versión más antigua del agente del directorio `/opt/ibm/ccm/agent`. Si desea eliminar todos los agentes, ejecute el mandato **`/opt/ibm/ccm/agent/bin/smai-agent.sh uninstall_all`**.
- Linux Si está actualizando agentes de FP6 o anterior, tras completar la actualización de los agentes a un nuevo directorio y la configuración o reconfiguración de los agentes, es posible que desee eliminar el directorio de instalación más antiguo. Complete estos pasos:

  1. En la máquina virtual o sistema donde se ha(n) instalado el agente (o agentes) de supervisión, inicie una línea de mandatos y vaya a la carpeta binaria en el directorio de instalación antiguo, `/opt/ibm/ccm/agent/bin`.
  2. Para desinstalar todos los agentes de supervisión instalados del directorio de instalación antiguo, escriba: `./smai-agent.sh uninstall_all`
  3. Suprima el directorio de instalación antiguo.

Conservación de los cambios de configuración del agente

Los usuarios avanzados pueden aplicar valores de alteración temporal a la personalización de componentes. Al aplicar valores de alteración temporal se garantiza que se conserven los valores durante una actualización. Primero pruebe los cambios en el entorno antes de aplicarlos globalmente.

Acerca de esta tarea

- Estas instrucciones son para los agentes de Linux y AIX. Encontrará una lista de códigos de producto de agente y los mandatos para detener e iniciar los agentes en "Utilización de mandatos de agente" en la página 184.
- El proceso agente de Windows conserva los cambios de configuración por diseño: las variables actualizadas en el archivo k*cp*cma.ini, donde *cp* es el código de producto, se mantienen en la sección Sustituir valores locales. Estas variables se utilizan en cada configuración para actualizar las entradas del registro de Windows que los agentes utilizan en tiempo de ejecución.
- Los valores personalizados del archivo *.cp*.environment y del archivo ..global.environment se pierden después de la actualización del agente. Para conservar los valores, realice los cambios de configuración en los archivos *cp*.environment y global.environment. La actualización del agente no sobrescribe los valores de estos archivos.

Procedimiento

Realice los pasos siguientes para guardar los cambios de configuración realizados en el archivo de entorno y conservarlos después de la actualización del agente:

1. Cree o actualice los archivos siguientes como sea necesario, donde *dir_instalación* es el directorio de instalación de agente (como el directorio /opt/ibm/apm/agent/ predeterminado de Linux o el directorio /opt/ibm/ccm/agent/ predeterminado de AIX):

Nombre de archivo	Descripción
***dir_instalación*/config/*cp*.environment**	*cp* en el nombre de archivo es el código de producto del agente, como mq o rz.
***dir_instalación*/config/global.environment**	Actualice el archivo de entorno global para que los cambios que desea afecten a todos los tipos de agente.

   Por ejemplo, as.environment es el archivo de entorno de Agente de WebSphere Applications permanente. .as.environment se sobrescribe cuando se actualiza el agente a una nueva versión.

   Defina las variables en el formato *clave=valor* donde *clave* es el nombre de variable de entorno y *valor* es el valor o el parámetro (como **KDC_FAMILIES=${KDC_FAMILIES}HTTP:10001**).
2. Después de acabar de actualizar los valores de variable, guarde y cierre el archivo de entorno y reinicie los agentes afectados.

Resultados

Las actualizaciones se aplican a todos los agentes del mismo tipo o, si ha actualizado el archivo de entorno global, a todos los agentes que informan al Servidor de Cloud APM. Los cambios permanecen con las actualizaciones de versión del agente.

Agentes en AIX: Detención del agente y ejecución de slibclean antes de actualizar

Si está actualizando un agente como usuario no root en sistemas AIX, debe completar esta tarea. Antes de ejecutar el instalador del agente, debe detener el agente y ejecutar **slibclean** para borrar la biblioteca libkududp.a.

Procedimiento

1. Detenga el agente ejecutando uno de los mandatos siguientes, según si el agente da soporte a varias instancias:
   - `./nombre-agent.sh stop`
   - `./nombre-agent.sh stop nombre_instancia`

   Consulte "Utilización de mandatos de agente" en la página 184.
2. Ejecute el siguiente mandato con privilegios de usuario root.

```
slibclean
```

Consulte Mandato slibclean en IBM Knowledge Center.

Resultados
El agente se ha detenido y la biblioteca `libkududp.a` se ha borrado.

Qué hacer a continuación
Ejecute el instalador del agente para actualizar el agente al release que ha descargado. Consulte Capítulo 6, “Instalación de los agentes”, en la página 125.Si la actualización falla, reinicie el servidor y repita el procedimiento.

Agente de HMC Base en AIX: Detención del agente como usuario no root y ejecución de `slibclean` antes de actualizar

Antes de actualizar el Agente de HMC Base como usuario no root en AIX, debe detener el Agente de HMC Base y ejecutar **slibclean** para borrar las bibliotecas dependientes de la memoria caché.

Acerca de esta tarea

Procedimiento

1. Ejecute el mandato siguiente como usuario no root para detener el agente.

   ```
   hmc_base-agent.sh stop
   ```

2. Ejecute el siguiente mandato con privilegios de usuario root.

   ```
   slibclean
   ```

   Consulte Mandato slibclean en IBM Knowledge Center.

Resultados
Se detiene el Agente de HMC Base y se borran las bibliotecas dependientes.

Qué hacer a continuación
Ejecute el instalador de agentes para actualizar el Agente de HMC Base.

Agente de Node.js: Eliminación de los plug-in de recopilador de datos antes de actualizar

Antes de actualizar el Agente de Node.js, debe eliminar los plug-in de supervisión de la aplicación Node.js.

Acerca de esta tarea
En función de la versión de Agente de Node.js, debe seguir diferentes procedimientos para eliminar los plug-ins de supervisión de la aplicación Node.js. Para averiguar cuál es la versión del agente, consulte Mandato de versión de agente.

Procedimiento

1. Eliminar plug-ins de recopilador de datos del principio del archivo de aplicación Node.js.
   - Si actualiza el Agente de Node.js de V01.00.12.00 a V01.00.13.00, siga este procedimiento:
     – Si ha habilitado la recopilación de datos de recurso, elimine la línea siguiente del principio del archivo de aplicación de Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_index.js');
       ```

donde *KNJ_NPM_LIB_LOCATION* es el directorio a la carpeta `lib` del directorio de instalación global del paquete npm. El directorio predeterminado es `/usr/local/lib`.

- Si ha habilitado la recopilación de datos de recurso y la recopilación de datos de diagnóstico detallado, elimine la línea siguiente del principio del archivo de aplicación Node.js:

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_deepdive.js');
```

- Si ha habilitado la recopilación de datos de recurso, la recopilación de datos de diagnóstico detallado y la recopilación de rastreos de método, elimine la línea siguiente del principio del archivo de aplicación Node.js:

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_methodtrace.js');
```

- Si actualiza el Agente de Node.js de V01.00.10.00 a V01.00.13.00, siga este procedimiento:
  - Si habilitó la recopilación de datos de recurso, elimine la línea siguiente del principio del archivo de aplicación de Node.js.

```
require('dir_instalación/lx8266/nj/bin/plugin/knj_index.js');
```

, donde *dir_instalación* es el directorio de instalación de Agente de Node.js.

  - Si ha habilitado la recopilación de datos de recurso y la recopilación de datos de diagnóstico detallado, elimine la línea siguiente del principio del archivo de aplicación Node.js.

```
require('dir_instalación/lx8266/nj/bin/plugin/knj_deepdive.js');
```

  - Si ha habilitado la recopilación de datos de recurso, la recopilación de datos de diagnóstico detallado y la recopilación de rastreos de método, elimine la línea siguiente del principio del archivo de aplicación Node.js.

```
require('dir_instalación/lx8266/nj/bin/plugin/knj_methodtrace.js');
```

2. Reinicie la aplicación Node.js para inhabilitar los plug-in de recopilador de datos.
   - Si la versión del Agente de Node.js actual es V01.00.10.00, hasta ahora los plug-ins de recopilador de datos se han eliminado satisfactoriamente.
   - Si la versión del Agente de Node.js actual es V01.00.12.00, vaya al paso siguiente.
3. Ejecute el mandato `./uninstall.sh` desde el directorio *dir_instalación*`/lx8266/nj/bin` para eliminar los valores de agente anteriores.

Qué hacer a continuación

Actualice el Agente de Node.js. Consulte “Actualización de los agentes” en la página 1173.

Agente de Supervisión de tiempo de respuesta: actualización de Módulo de Tiempo de respuesta de IBM HTTP Server

Si anteriormente supervisaba IBM HTTP Server utilizando Módulo de Tiempo de respuesta de IBM HTTP Server o Agente de HTTP Server, actualice la instalación.

Acerca de esta tarea

La tabla siguiente muestra algunos escenarios de instalación que pueden ser similares a la forma como supervisa IBM HTTP Server.

agente Supervisión de tiempo de respuesta	Utilización de Módulo de Tiempo de respuesta de IBM HTTP Server?	Utilización de Analizador de paquetes?	¿Agente de HTTP Server está instalado?
AIX y xLinux: 08.11.00 y posteriores Windows: 08.14.02 y posteriores	✓	—	✓
AIX y xLinux: 08.10.00	✓	—	—
AIX y xLinux: 08.10.00	✓	—	✓
7.40.07 o anterior	—	✓	—
7.40.07 o anterior	—	✓	✓

Para todos estos escenarios, el proceso de instalación es parecido.

Procedimiento

1. Instale Agente de HTTP Server desde el release V8.1.1 o posterior en AIX o Linux; desde el release V8.1.4.02 o posterior en Windows.

   El Módulo de Tiempo de respuesta de IBM HTTP Server se instala automáticamente con el agente.
2. Configure el Agente de HTTP Server.

   Nota: Si anteriormente estaba usando Módulo de Tiempo de respuesta de IBM HTTP Server, actualice el archivo de configuración del servidor web (`httpd.conf`) con la ubicación del nuevo Módulo de Tiempo de respuesta de IBM HTTP Server y elimine el antiguo archivo de configuración de módulo de carga (`mod_wrt.so`).

   Nota: El agente de Supervisión de tiempo de respuesta V8.1.1 y posteriores no funciona con el archivo de módulo de carga (`mod_wrt.so`) de releases anteriores. Si intenta utilizar una versión anterior de este archivo, se crearán mensajes de registro de error. Las transacciones quizá puedan seguir rastreándose pero los datos de instancia de transacción no se visualizarán.

   Para más información, consulte el PDF de referencia de Agente de HTTP Server, que puede descargar desde http://ibm.biz/agent-httpserver.
3. Asegúrese de que IBM HTTP Server y Agente de HTTP Server estén ejecutando. Si el instalador de Supervisión de tiempo de respuesta detecta Agente de HTTP Server, el agente de Supervisión de tiempo de respuesta habilitará Módulo de Tiempo de respuesta de IBM HTTP Server en lugar de Analizador de paquetes.
4. Instale el agente Supervisión de tiempo de respuesta en la misma ubicación `AGENT_HOME` que el Agente de HTTP Server.
   - Linux AIX Instale V8.1.1 o posterior como **`root`**. Ejemplo de `AGENT_HOME /opt/ibm/apm/agent/`
   - Windows Instale V8.1.4.0.2 o posterior con permisos de administrador. Ejemplo de `AGENT_HOME C:\IBM\APM\`.
5. Si utilizaba el Analizador de paquetes en releases anteriores, es posible que tenga que inhabilitar el Analizador de paquetes para empezar a supervisar IBM HTTP Server con Módulo de Tiempo de respuesta de IBM HTTP Server.
6. Reinicie el IBM HTTP Server.

Agente de Microsoft .NET: Eliminación del recopilador de datos .NET antes de actualizar

Antes de actualizar el Agente de Microsoft .NET, debe eliminar el recopilador de datos .NET de las aplicaciones .NET.

Procedimiento

1. Anular el registro de todos los módulos del recopilador de datos.
   Como administrador, escriba:

   ```
   cd dir_instalación\qe\bin configdc unregisterdc all
   ```

   Donde *dir_instalación* es el directorio de instalación del Agente de Microsoft .NET.
2. Reinicie las aplicaciones .NET.

Qué hacer a continuación

Actualice el Agente de Microsoft .NET. Consulte "Actualización de los agentes" en la página 1173.

Agente de OpenStack: Reconfiguración de instancias de agente para utilizar la API de identidad de OpenStack v3

Para actualizar el Agente de OpenStack para utilizar la API de identidad de OpenStack v3, después de instalar la última versión del agente, debe reconfigurar todas las instancias del agente y actualizar el archivo de configuración del recopilador de datos.

Acerca de esta tarea

Esta tarea sólo es obligatoria cuando se actualiza el agente para utilizar la API de identidad de OpenStack v3.

Procedimiento

1. Reconfigure todas las instancias de agente existentes. Para obtener instrucciones detalladas, consulte "Configuración del Agente de OpenStack" en la página 633.
2. Busque el archivo de configuración del recopilador de datos de agentes ksg_dc_*nombre_instancia*.cfg, donde *nombre_instancia* es el nombre especificado para esta instancia de agente.
   Si el archivo no existe, copie *dir_instalación*/lx8266/sg/bin/ksg_dc.cfg en el directorio *dir_instalación*/config y cambie el nombre de archivo a ksg_dc_*nombre_instancia*.cfg.
   Por ejemplo, si el nombre de instancia es OS1, cambie el nombre a ksg_dc_OS1.cfg.
3. Añada la sección siguiente al archivo ksg_dc_*nombre_instancia*.cfg:

   ```
   #OpenStack authentication information
   [OS_authentication_info]
   OS_project_domain_name=Default
   OS_user_domain_name=Default
   OS_cert_path=
   ```

4. Reinicie la instancia del agente ejecutando los mandatos siguientes:

   ```
   dir_instalación/bin/openstack-agent.sh stop nombre_instancia
   dir_instalación/bin/openstack-agent.sh start nombre_instancia
   ```

   donde *nombre_instancia* es el nombre de la instancia de agente que debe configurarse.

Agente de Ruby: Eliminación de los plug-in de recopilador de datos antes de actualizar

Antes de actualizar el Agente de Ruby, debe eliminar los plug-in de supervisión de la aplicación Ruby.

Procedimiento

1. Elimine el recopilador de datos de la versión anterior ejecutando el mandato siguiente.

   ```
   gem uninstall stacktracer
   ```

2. Vaya al directorio de inicio de la aplicación, abra su Gemfile, y elimine la línea siguiente: gem 'stacktracer', '*versión*'

Donde *versión* es el número de versión del Agente de Ruby.

3. En el directorio de inicio de la aplicación, especifique: `bundle install`

Qué hacer a continuación

Actualice el Agente de Ruby. Consulte "Actualización de los agentes" en la página 1173.

Agente de WebSphere Applications: Migración del recopilador de datos

Tras actualizar el agente, debe migrar el recopilador de datos de forma interactiva o en modalidad silenciosa.

Migración interactiva del recopilador de datos

Puede migrar un nivel de mantenimiento anterior del recopilador de datos de forma interactiva mediante el programa de utilidad de migración.

Antes de empezar

Linux AIX Si ha instalado WebSphere Application Server o WebSphere Portal Server utilizando una cuenta de usuario no root, antes de ejecutar los programas de utilidad de configuración, verifique que el usuario no root tiene privilegios de lectura y grabación en los siguientes directorios de agente en *dir_instalación*/yndchome/7.3.0.14.08, donde *dir_instalación* es el directorio de instalación del Agente de WebSphere Applications:

- `data`
- `bin`
- `runtime`
- `logs`

Proporcione permisos de lectura y grabación mediante el mandato `chmod 777`, según se requiera. Además, inicie sesión como el usuario que se ha utilizado para instalar el servidor de aplicaciones.

Acerca de esta tarea

Puede migrar un nivel de mantenimiento anterior del recopilador de datos de forma interactiva mediante el programa de utilidad de migración. Si desea migrar varias instancias de servidor de aplicaciones, es posible que sea más conveniente utilizar el programa de utilidad de migración en modalidad silenciosa.

Importante:

- Sólo puede migrar niveles de mantenimiento anteriores de la versión 7.3 de un recopilador de datos. La versión del recopilador de datos se indica en la vía de acceso del directorio de inicio del recopilador de datos.
- No se puede migrar desde la versión 7.3 del recopilador de datos a la versión 7.3 fixpack 1. En lugar de ello, desconfigure el recopilador de datos y desinstale la versión 7.3 del agente. A continuación, instale la versión 7.3 fixpack 1 del agente y configure de nuevo el recopilador de datos.

Procedimiento

1. Linux AIX Inicie la sesión con el usuario que se ha utilizado para instalar el servidor de aplicaciones.
2. Inicie el programa de utilidad de migración desde el directorio de instalación de la versión más reciente del agente.

   Linux AIX Ejecute el mandato *dir_inicio_dc*`/bin/migrate.sh`

   Windows Ejecute el mandato *dir_inicio_dc*`\bin\migrate.bat`
3. El programa de utilidad muestra las direcciones IP de todas las tarjetas de red que se encuentran en el sistema local.

Especifique el número que corresponda a la dirección IP que se va a utilizar.

4. El programa de utilidad descubre todos los servidores configurados por niveles de mantenimiento anteriores del recopilador de datos y los presenta en una lista. Los recopiladores de datos se agrupan por nivel de mantenimiento.

   Seleccione una o más instancias de servidor de aplicaciones de la lista.

   La lista podría incluir tanto instancias de servidor WebSphere tradicional como de servidores Liberty. Las instancias de servidor WebSphere tradicional podrían estar en distintos perfiles.

   Consejo:

   - Si se supervisan varias instancias bajo un solo perfil, debe seleccionarlas todas para migrarlas simultáneamente.
   - Migre todos los servidores bajo el perfil de Liberty simultáneamente. La migración parcial de los servidores configurados podría causar inestabilidad.

   Recuerde:

   - Para un entorno autónomo, las instancias de servidor de aplicaciones se deben estar ejecutando.
   - Para un entorno de Network Deployment, el agente de nodo y el gestor de despliegue deben estar en ejecución.
   - No es necesario que los servidores Liberty estén en ejecución durante la migración.
5. Especifique el número que corresponda a la instancia de servidor de aplicaciones cuyo recopilador de datos se va a migrar o especifique un asterisco (*) para migrar el recopilador de datos de todas las instancias de servidor de aplicaciones.

   Para especificar un subconjunto de servidores, especifique los números, separados por comas, que representan los servidores. Por ejemplo: `1,2,3`.

   El programa de utilidad de migración integra automáticamente cada recopilador de datos con el agente de supervisión. Los valores de puerto y host de agente de supervisor se recuperan de los archivos de configuración existentes.
6. Especifique un alias para cada uno de los servidores seleccionados.

   El valor predeterminado es el alias de servidor existente.
7. Para la instancia de servidor de Liberty, especifique el directorio de inicio de JVM cuando se le solicite. Por ejemplo, `/opt/IBM/java`.
8. El programa de utilidad determina si la seguridad global de WebSphere está habilitada para cada uno de los perfiles donde se está migrando la recopilación de datos.

   Si la seguridad global de WebSphere está habilitada para uno o más perfiles, especifique si desea recuperar los valores de seguridad de un archivo de propiedades de cliente:

   El recopilador de datos se comunica con los Servicios administrativos de WebSphere utilizando RMI o el protocolo SOAP. Si la seguridad global está habilitada para un perfil, debe especificar el ID de usuario y la contraseña de un usuario que tenga autorización para iniciar sesión en la consola administrativa de IBM WebSphere Application Server para el perfil.

   O bien, puede cifrar el nombre de usuario y la contraseña y almacenarlos en archivos de propiedades de cliente de servidor de aplicaciones antes de configurar el recopilador de datos. Debe utilizar el archivo `sas.client.props` para una conexión RMI o el archivo `soap.client.props` para una conexión SOA.
9. Especifique 1 para permitir que el programa de utilidad recupere el nombre de usuario y la contraseña del archivo de propiedades de cliente correspondiente y pasar al paso “11” en la página 1183. De lo contrario, especifique 2 para especificar el nombre de usuario y la contraseña.

   Importante: La conexión a la consola administrativa de WebSphere Application Server puede tardar bastante.
10. Especifique el nombre de usuario y la contraseña para cada perfil si la seguridad global de WebSphere está habilitada.

11. El programa de utilidad migra la recopilación de datos para cada instancia de servidor de aplicaciones seleccionada. Muestra un mensaje de estado que indica si la migración de cada servidor se ha completado satisfactoriamente.
12. Reinicie las instancias según indique el programa de utilidad. La configuración del recopilador de datos se aplica cuando se reinician las instancias de servidor de aplicaciones.

Resultados
El recopilador de datos se migra al último nivel de mantenimiento instalado.

Qué hacer a continuación
El programa de utilidad de migración conserva los valores que se han configurado en la versión anterior del recopilador de datos. Para modificar estos valores, puede ejecutar el programa de utilidad de configuración o reconfiguración en la modalidad interactiva o silenciosa desde el directorio *dir_inicio_dc*\bin del nuevo recopilador de datos. Para obtener más información, consulte "Configuración o reconfiguración del recopilador de datos con los programas de utilidad de configuración completa" en la página 869.

Migración del recopilador de datos en modalidad silenciosa
Puede migrar un nivel de mantenimiento anterior del recopilador de datos mediante el programa de utilidad de migración en modalidad silenciosa.

Antes de empezar

Linux AIX Si ha instalado WebSphere Application Server o WebSphere Portal Server utilizando una cuenta de usuario no root, antes de ejecutar los programas de utilidad de configuración, verifique que el usuario no root tiene privilegios de lectura y grabación en los siguientes directorios de agente en *dir_instalación*/yndchome/7.3.0.14.08, donde *dir_instalación* es el directorio de instalación del Agente de WebSphere Applications:

- data
- bin
- runtime
- logs

Proporcione permisos de lectura y grabación mediante el mandato chmod 777, según se requiera. Además, inicie sesión como el usuario que se ha utilizado para instalar el servidor de aplicaciones.

Acerca de esta tarea
Se suministra un archivo de propiedades silencioso de ejemplo, sample_silent_migrate.txt, con el programa de utilidad de migración. El archivo está disponible en el directorio *dir_instalación*/yndchome/7.3.0.14.08/bin.

Al crear el archivo de propiedades silencioso, tenga en cuenta las consideraciones siguientes:

- Una línea en el archivo que empieza con un signo de número (#) se trata como un comentario y no se procesa. Si el signo de número se utiliza en cualquier otra posición de la línea, no se considera el inicio de un comentario. Esto significa que puede utilizar el signo de número en contraseñas o para otros usos.
- Cada propiedad se describe en una línea distinta, en el siguiente formato: propiedad = valor.

  propiedad
  Es el nombre de la propiedad. La lista de propiedades válidas que puede configurar se muestra en la Tabla 256 en la página 1184. No modifique ni elimine propiedades del archivo de ejemplo que no aparezcan en la tabla.

  valor
  Es el valor de la propiedad. Ya se han proporcionado valores predeterminados para algunas propiedades. Puede suprimir los valores predeterminados para dejar los valores de propiedades en blanco o vacíos. Un valor vacío se trata como si la propiedad no se hubiera especificado, en vez de

utilizar el valor predeterminado. Si desea utilizar valores predeterminados, marque como comentario la propiedad en el archivo.

- Las contraseñas están en texto sin formato.
- Las propiedades y los valores distinguen entre mayúsculas y minúsculas.

Tabla 256 en la página 1184 describe las propiedades que están disponibles al migrar el recopilador de datos en modalidad silenciosa.

Tabla 256. Propiedades disponibles para ejecutar el programa de utilidad de migración en modalidad silenciosa

Propiedad	**Comentario**
migrate.type	Debe ser AD.
default.hostip	Si el sistema utiliza varias direcciones IP, especifique la dirección IP que debe utilizar el recopilador de datos.
itcam.migrate.home	Especifica el directorio de inicio del recopilador de datos de la versión de mantenimiento anterior del recopilador de datos. El directorio no se suprime como parte de la migración.
was.wsadmin.connection.host	Especifica el nombre del host al que se está conectando la herramienta wsadmin. En un entorno de Network Deployment, especifique la conexión wsadmin al gestor de despliegue. En un entorno autónomo, especifique la conexión wsadmin con el servidor.
was.wsadmin.username	Especifica el ID de un usuario con autorización para iniciar una sesión en la consola administrativa de IBM WebSphere Application Server. Este usuario debe tener el rol de agente en el servidor de aplicaciones.
was.wsadmin.password	Especifica la contraseña que corresponde al usuario especificado en la propiedad `was.wsadmin.username`.
was.appserver.profile.name	Especifica el nombre del perfil del servidor de aplicaciones que desea configurar. **Recuerde:** La propiedad no es necesaria para un perfil de Liberty.
was.appserver.home	Especifica el directorio de inicio de WebSphere Application Server.
was.appserver.cell.name	Especifica el nombre de célula de WebSphere Application Server. **Recuerde:** La propiedad no es necesaria para un perfil de Liberty.
was.appserver.node.name	Especifica el nombre de nodo de WebSphere Application Server. **Recuerde:** La propiedad no es necesaria para un perfil de Liberty.

Tabla 256. Propiedades disponibles para ejecutar el programa de utilidad de migración en modalidad silenciosa (continuación)	
Propiedad	**Comentario**
was.appserver.server.name	Especifica la instancia de servidor de aplicaciones del perfil del servidor de aplicaciones que se debe migrar a la nueva versión del recopilador de datos. El archivo de propiedades silencioso puede tener varias instancias de esta propiedad.

Importante:

- Sólo puede migrar niveles de mantenimiento anteriores de la versión 7.3 de un recopilador de datos. La versión del recopilador de datos se indica en la vía de acceso del directorio de inicio del recopilador de datos.
- No se puede migrar desde la versión 7.3 del recopilador de datos a la versión 7.3 fixpack 1. En lugar de ello, desconfigure el recopilador de datos y desinstale la versión 7.3 del agente. A continuación, instale la versión 7.3 fixpack 1 del agente y configure de nuevo el recopilador de datos.

Procedimiento

1. Especifique las opciones de configuración en el archivo de migración silenciosa.
2. Ejecute el mandato para iniciar el programa de utilidad de migración en modalidad silenciosa desde el directorio de instalación de la versión más reciente del agente.
   - Linux AIX `dir_inicio_dc/bin/migrate.sh -silent nombre_archivo_migración_silenciosa_ejemplo`
   - Windows `dir_inicio_dc\bin\migrate.bat -silent nombre_archivo_migración_silenciosa_ejemplo`

Resultados
El recopilador de datos se migra al último nivel de mantenimiento instalado.

Qué hacer a continuación
El programa de utilidad de migración conserva los valores que se han configurado en la versión anterior del recopilador de datos. Para modificar estos valores, puede ejecutar el programa de utilidad de configuración o reconfiguración en la modalidad interactiva o silenciosa desde el directorio *dir_inicio_dc*\bin del nuevo recopilador de datos. Para obtener más información, consulte "Configuración o reconfiguración del recopilador de datos con los programas de utilidad de configuración completa" en la página 869.

Agente de Tomcat: Actualización de la infraestructura principal de TEMA en Windows

Para actualizar la infraestructura principal de TEMA en Windows para Agente de Tomcat, debe tener el agente y el servidor para actualizar correctamente la infraestructura de TEMA.

Procedimiento

1. Prepare la configuración del servidor Tomcat.
2. Instale y configure el agente de Tomcat.
3. Inicie la sesión en el panel de instrumentos de IBM Cloud Application Performance Management, vaya a **Configuración del agente** > **Tomcat**, seleccione una instancia de Agente de Tomcat y pulse **Habilitar TT/DD**.
4. Reinicie el servidor Tomcat.
5. Para aplicar IBM APM CORE FRAMEWORK, detenga el servidor y el agente Tomcat.
6. Vaya a TEMA/<IBM APM CORE FRAMEWORK_HOME>. Ejecute el mandato

apmpatch.bat <directorio de instalación del agente de Tomcat>.
La infraestructura se actualiza.

7. Compruebe la versión de la infraestructura principal de IBM APM actualizada ejecutando las instrucciones siguientes.
   `Goto <dir_instalación_agente_TOMCAT>\InstallITM`
   `Run: KinCInfo.exe -i`.
8. Inicie el servidor y el agente de Tomcat.

Actualización de los recopiladores de datos

De forma periódica, hay nuevos archivos de archivado que contienen recopiladores de datos actualizados disponibles para su descarga. Los archivos de archivado están disponibles en Productos y servicios, en el sitio web de IBM Marketplace..

Antes de empezar

Acerca de esta tarea

Para actualizar un recopilador de datos, siga estos pasos:

Procedimiento

- Desconfigure el recopilador de datos de las aplicaciones locales y/o IBM Cloud:
  - Para el Recopilador de datos de J2SE, no se necesitan pasos de desconfiguración.
  - Para el Recopilador de datos de Liberty, siga las instrucciones de "Desconfiguración del recopilador de datos para aplicaciones IBM Cloud" en la página 922 y/o "Desconfigurar el recopilado de datos para aplicaciones locales" en la página 915.
  - Para el Recopilador de datos de Node.js, siga las instrucciones de "Desconfiguración del Recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud" en la página 621 y/o "Desconfiguración del Recopilador de datos de Node.js autónomo para aplicaciones locales" en la página 627.
  - Para el Recopilador de datos de Python, siga las instrucciones de "Desconfiguración del Recopilador de datos de Python para aplicaciones de IBM Cloud" en la página 700 y/o "Desconfiguración del Recopilador de datos de Python para aplicaciones locales" en la página 706.
  - Para el Recopilador de datos de Ruby, siga las instrucciones de "Desconfiguración del Recopilador de datos de Ruby para aplicaciones de IBM Cloud" en la página 755.
- Descargue el paquete del recopilador de datos.
- Vuelva a configurar el recopilador de datos para supervisar las aplicaciones locales y/o IBM Cloud:
  - Para el Recopilador de datos de Node.js, después de actualizar el recopilador de datos, vuelva a configurarlo. Para obtener instrucciones, consulte las secciones "Configuración del Recopilador de datos de Node.js autónomo para aplicaciones IBM Cloud (anteriormente Bluemix)" en la página 615 y/o "Configuración del Recopilador de datos de Node.js autónomo para aplicaciones locales" en la página 621.
  - Para el Recopilador de datos de Python, después de actualizar el recopilador de datos, vuelva a configurarlo. Para obtener instrucciones, consulte las secciones "Configuración del recopilador de datos de Python para aplicaciones IBM Cloud" en la página 695 y/o "Configuración del Recopilador de datos de Python para aplicaciones locales" en la página 701.
  - Para el Recopilador de datos de Liberty, después de actualizar el recopilador de datos, vuelva a configurarlo. Para obtener instrucciones, consulte las secciones "Configuración del recopilador de datos de Liberty para aplicaciones IBM Cloud" en la página 916 y/o "Configuración del recopilador de datos para aplicaciones locales" en la página 912.

- Para el Recopilador de datos de J2SE, después de actualizar el recopilador de datos, vuelva a configurarlo. Para obtener instrucciones, consulte “Configuración de la supervisión de J2SE” en la página 468.
- Para el Recopilador de datos de Ruby, después de actualizar el recopilador de datos, vuelva a configurarlo. Para obtener instrucciones, consulte “Configuración del Recopilador de datos de Ruby para aplicaciones de IBM Cloud” en la página 751.

Resultados
El recopilador de datos se actualiza a la última versión.

Capítulo 12. Resolución de problemas y soporte

Revise las entradas de resolución de problemas para los problemas que podría experimentar al instalar, configurar o utilizar IBM Cloud Application Performance Management.

El contenido de la resolución de problemas está disponible en este Knowledge Center. Anteriormente, el contenido de resolución de problemas estaba disponible en el Foro de Cloud Application Performance Management en developerWorks. Puede continuar buscando entradas anteriores en este foro. Busque entradas que empiecen por "Resolución de problemas".

Para la resolución de problemas de IBM Cloud Application Performance Management Hybrid Gateway, consulte “Gestión de la Pasarela híbrida” en la página 997.

Resolución de problemas de los agentes

Resolución de problemas de instalación y configuración del agente de .

Estamos migrando el contenido de resolución de problemas desde el Foro de Cloud Application Performance Management en developerWorks a este Knowledge Center. Anteriormente, el contenido de resolución de problemas estaba disponible en el Foro de Cloud Application Performance Management en developerWorks. Puede continuar buscando entradas anteriores en este foro. Busque entradas que empiecen por "Resolución de problemas".

Internet Service Monitoring

Puede encontrar aquí más detalles sobre los problemas conocidos de Internet Service Monitoring.

El perfil no se creará después de que crear página de perfil se haya mantenido abierto durante más de 10 minutos y no se creará otro perfil con el mismo nombre

Problema

El perfil no se creará después de que **crear página de perfil** se haya mantenido abierto durante más de 10 minutos y no se creará otro perfil con el mismo nombre.

Síntoma

Al crear un perfil si el usuario mantiene **crear página de perfil** desocupado (abierto sin ninguna actividad) durante más de 10 minutos y, a continuación, intenta crear el perfil, éste no se creará. Después de eso, si el usuario intenta volver a crear el perfil con el mismo nombre, el perfil no se creará.

Causa

Se crea un archivo de bloqueo en el lado MIN en el momento de la creación del perfil que bloquea la actividad de la creación del perfil para el mismo perfil para otros usuarios. El archivo de bloqueo se suprime después de que se haya realizado la creación del perfil. Pero si la ventana de creación está desocupada durante más de 10 minutos, el suceso de creación se bloquea y el usuario no podrá crear el perfil.

Solución

- El usuario no debe mantener la ventana desocupada durante más de 10 minutos al crear un perfil.
- El administrador puede suprimir el archivo de bloqueo del perfil que se ha creado desde el lado MIN en `/opt/ibm/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/data_source/is`.
  Por ejemplo, si el nombre de perfil es ABC, se crea un archivo de bloqueo `$$ABC$$1UjQ9wy1boIHTAQeoWSj1IU.lock`.

Supervisión de Microsoft Active Directory

Puede encontrar aquí más detalles sobre los problemas conocidos de la supervisión de Microsoft Active Directory.

El agente de Microsoft Active Directory no muestra contenido de ayuda en línea actualizado

Problema

Las páginas de ayuda en línea no se han actualizado con el último contenido para el agente de Microsoft Active Directory.

Síntoma

En la ayuda de Eclipse del panel de instrumentos de APM para Agente de Microsoft Active Directory, falta el contenido de la ayuda para el intervalo de recopilación de datos y el periodo de retención de los siguientes grupos de atributos recién añadidos:

- Servicios de directorio
- Kerberos Consistency Checker
- Centro de distribución de claves Kerberos
- Proveedor de servicio de nombres
- Servicio de directorio de Exchange

Causa

El problema se produce debido a la restricción en el servidor de compilación.

Solución

El usuario puede encontrar el contenido de la ayuda en la respectiva ayuda contextual de los grupos de atributos en el panel de instrumentos de APM.

Nota: El problema aparece en el release de APM V8.1.4.10.

Supervisión de Microsoft IIS

Puede encontrar aquí más detalles sobre los problemas conocidos de Microsoft Internet Information Services.

Las páginas de ayuda en línea no se actualizan con el contenido más reciente para el agente de APM de Microsoft IIS

Problema

Las páginas de ayuda en línea no se actualizan con el contenido más reciente para el agente de APM de Microsoft IIS

Síntoma

Faltan los grupos de atributos recién añadidos en el contenido de la ayuda en línea:

- WPROCESS
- MEMIISUS
- Recogida de basura de ASP
- IISSVRINFO

Causa

Este problema se está produciendo debido a problemas de servidor de compilación.

Solución temporal

No disponible. Sin embargo puede ver el contenido de la ayuda del grupo de atributos concreto en el panel de instrumentos de APM.

Supervisión de Microsoft .NET

Puede encontrar aquí más detalles sobre los problemas conocidos de la supervisión de Microsoft .NET.

El agente de Microsoft .NET no muestra el contenido de la ayuda en línea actualizado

Problema

Las páginas de ayuda en línea no se actualizan con el contenido más reciente de Agente de Microsoft .NET.

Síntoma

En la ayuda de Eclipse del panel de instrumentos de APM para Agente de Microsoft .NET, falta el contenido de la ayuda del atributo Nombre de solicitud bajo el grupo de atributos Detalles de llamadas a base de datos.

Causa

El problema se produce debido a la restricción en el servidor de compilación.

Solución

El usuario puede encontrar el contenido de ayuda en la ayuda contextual del widget de grupo de atributos Detalles de llamadas a base de datos en el panel de instrumentos de APM.

Nota: El problema aparece en el release de APM V8.1.4.10.

Supervisión de Microsoft SharePoint Server

Puede encontrar aquí más detalles sobre los problemas conocidos de supervisión de Microsoft SharePoint Server.

El agente de Microsoft SharePoint Server no muestra contenido de ayuda en línea actualizado

Problema

Las páginas de ayuda en línea no se actualizan con el contenido más reciente de Agente de Microsoft SharePoint Server.

Síntoma

En la ayuda de Eclipse del panel de instrumentos de APM para Agente de Microsoft SharePoint Server, falta el contenido de ayuda para los widgets de grupo recién añadidos denominados `Recuento del registro de rastreo de la última 1 hora` y `Detalles de registro de rastreo`.

Causa

El problema se produce debido a la restricción en el servidor de compilación.

Solución

El usuario puede encontrar el contenido de la ayuda en la ayuda contextual de los respectivos widgets de grupo en el panel de instrumentos de APM.

Nota: El problema aparece en el release de APM V8.1.4.10.

Supervisión de PostgreSQL

Puede encontrar aquí más detalles sobre los problemas conocidos de la supervisión de PostgreSQL.

El widget de porcentaje de coincidencias del almacenamiento intermedio para las bases de datos sin conexiones activas no muestra el contenido de la ayuda

Problema

La información no está disponible para las bases de datos que no tienen conexiones activas.

Síntoma

Las bases de datos sin conexiones activas no se visualizan en el widget de porcentaje de coincidencias del almacenamiento intermedio. La información debe mostrarse en el contenido de la ayuda del widget.

Causa

Limitación debido a la compatibilidad con IBM Cloud App Management.

Solución

No está disponible. El usuario debe tener en cuenta la limitación.

Los valores de memoria y dirección IP no se visualizan en la plataforma SUSE15

Problema

Los valores de memoria y dirección IP no se visualizan cuando el agente está supervisando el servidor PostgreSQL localmente en la plataforma SUSE15.

Síntoma

Los valores de memoria y dirección IP no se visualizan si el agente está supervisando el servidor PostgreSQL en la plataforma SUSE15.

Causa

El mandato **`netstat`** falla para el agente en la plataforma SUSE15.

Solución

El usuario puede utilizar la plataforma SUSE12 para supervisar el servidor PostgreSQL localmente.

Recopilación de registros de agente de supervisión para el equipo de soporte de IBM

Utilice la herramienta de recopilación de determinación de problemas, *pdcollect*, para recopilar los registros necesarios y otra información sobre la determinación de problemas solicitada por IBM Support para los agentes de supervisión. La herramienta del recopilador de PD se instala con cada agente de supervisión.

Antes de empezar
El permiso de administrador o raíz es necesario para la herramienta del recopilador de PD para recopilar información del sistema de los agentes de supervisión. Puede revisar los registros de agente individualmente en las carpetas siguientes:

- Windows [64 bits] *dir_instalación*\TMAITM6_x64\logs
- Windows [32 bits] *dir_instalación*\TMAITM6\logs

- Linux AIX *dir_instalación*/logs

Restricción: Solo es posible ejecutar una instancia del script pdcollect.

Acerca de esta tarea

La ubicación predeterminada de *dir_instalación* es:

- Windows C:\IBM\APM
- Linux /opt/ibm/apm/agent
- AIX /opt/ibm/apm/agent

Para ejecutar la herramienta de recopilador de PD, siga estos pasos:

Procedimiento

1. En la línea de mandatos, vaya al directorio del agente:
   - Linux AIX *dir_instalación*/bin
   - Windows *dir_instalación*\BIN
2. Ejecute el mandato siguiente:
   - Linux AIX **./pdcollect**
   - Windows **pdcollect**

   Se generará un archivo con una indicación de fecha y hora en el nombre de archivo en el directorio tmp, como por ejemplo /tmp/pdcollect-nc049021.tar.Z.
3. Envíe los archivos de salida a su representante de IBM Support.

Qué hacer a continuación

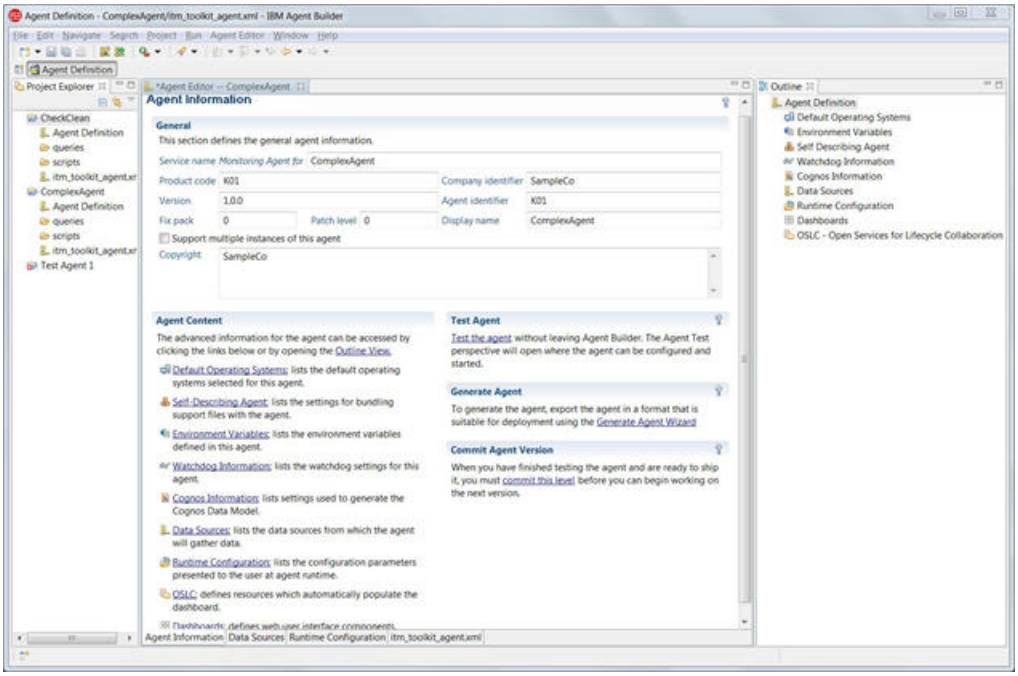
Si ha instalado el Agente de Ruby y lo ha configurado para los paneles de instrumentos de Diagnostics, ejecute la herramienta de recopilador, *kkmCollector*, en sistemas Linux para recopilar archivos de configuración, archivos de salida como, por ejemplo, archivos JSO, y archivos de registro.

1. Vaya al directorio *dir_instalación*/lx8266/km/bin.
2. Ejecute el mandato **./kkmCollector**

   Se genera un archivo con indicación de fecha y hora en el nombre de archivo en el directorio tmp, como por ejemplo /tmp/kkm_dchome.tar.gz
3. Envíe los archivos de salida a su representante de IBM Support.

Capítulo 13. Agent Builder

La herramienta IBM Agent Builder proporciona una interfaz de usuario gráfica para ayudarle a crear, modificar, depurar y empaquetar agentes para supervisar orígenes de datos en IBM Cloud Application Performance Management.



Descripción general de Agent Builder

Puede utilizar IBM Agent Builder para crear y modificar agentes personalizados que amplían las prestaciones de supervisión de un entorno IBM Tivoli Monitoring o IBM Cloud Application Performance Management. Un agente personalizado utiliza cualquiera de estos entornos para supervisar cualquier tipo de software de desarrollo propio o personalizado.

Agent Builder se basa en Eclipse, un entorno de desarrollo integrado de código abierto.

Agent Builder incluye las características siguientes para los entornos Tivoli Monitoring y Cloud APM:

Definir y modificar agentes
Pueden crearse y modificarse agentes. Los agentes recopilan y analizan datos sobre el estado y rendimiento de distintos recursos como, por ejemplo, discos, memoria, procesador o aplicaciones y proporcionan dichos datos al entorno de supervisión.

Probar y preparar agentes para su despliegue
Se puede probar un agente en Agent Builder recopilando datos en el host donde ejecuta Agent Builder (en algunos casos también se puede recopilar información de un host distinto). Puede empaquetarse el agente para facilitar su distribución y despliegue.

Las características adicionales siguientes están disponibles en Tivoli Monitoring:

Mandatos de actuación, situaciones y espacios de trabajo personalizados
Agent Builder puede usarse para empaquetar comandos de actuación, situaciones y espacios de trabajo adicionales con un agente nuevo o existente que ejecute en el entorno de Tivoli Monitoring

Modelos de datos de informes
Puede utilizar Agent Builder para generar un modelo de datos de Cognos que pueda utilizar para crear informes de Tivoli Common Reporting. Estos informes se pueden empaquetar como parte de su imagen de agente.

Procedimientos comunes de Agent Builder

La tabla siguiente lista los procedimientos principales que puede completar con Agent Builder.

Puede utilizar el Agent Builder para crear agentes para los entornos IBM Tivoli Monitoring e IBM Cloud Application Performance Management. También puede utilizarlo para crear extensiones de soporte de aplicaciones para el entorno Tivoli Monitoring. Las extensiones de soporte de aplicación se crean mediante la creación de espacios de trabajo y situaciones para mejorar uno o más agentes ya existentes.

Para utilizar Agent Builder, primero debe instalarlo. Para obtener instrucciones, consulte "Instalación e inicio de Agent Builder" en la página 1200.

Para crear, probar y utilizar un agente, complete los procedimientos de la tabla siguiente por el orden de lista.

Tabla 257. Información de consulta rápida para crear agentes

Objetivo	**Consulte**
Crear un agente utilizando el asistente de **Agente**.	• "Crear un agente" en la página 1205
Crear orígenes de datos y atributos para el agente. **Importante:** Para un entorno Cloud APM, un panel de instrumentos de resumen puede mostrar hasta cinco atributos aproximadamente; uno de los atributos debe denotar el estado general del agente o subnodo.	• "Edición del origen de datos y propiedades de atributos" en la página 1228
Para el entorno Tivoli Monitoring, crear espacios de trabajo y situaciones para el agente. • Ejecutar al menos de Tivoli Monitoring Versión 6.1 fixpack 1 • Establecer la versión de la solución Tivoli Universal Agent de nuevo en "00" • Establecer el valor para "AppTag"	• "Creación de espacios de trabajo, mandatos de Actuación y situaciones" en la página 1408 • "Importación de archivos de soporte de aplicaciones" en la página 1444
Para el entorno Cloud APM, crear definiciones de recursos y paneles de instrumentos para el agente.	• "Preparación del agente para Cloud APM" en la página 1414
Para el entorno Tivoli Monitoring, crear modelos de datos Cognos para informes para el agente.	• "Generación del modelo de datos de Cognos" en la página 1515
Probar y depurar el agente creado, garantizando la disponibilidad de la información de supervisión.	• "Pruebas del agente en Agent Builder" en la página 1417 • "Opciones de línea de mandatos" en la página 1454 • "Utilización del editor del agente para modificar el agente" en la página 1208.
Generar un paquete de instalación e instalar el agente en el host supervisado.	• "Instalación de un agente" en la página 1426
Eliminar un agente que ha creado con Agent Builder.	• "Desinstalación de un agente" en la página 1442

Puede utilizar también Agent Builder para empaquetar espacios de trabajo, situaciones y mandatos de actuación personalizados como extensiones de soporte de la aplicación para agentes existentes. Estas funciones solo están disponibles para el entorno Tivoli Monitoring:

Tabla 258. Información de consulta rápida para otras funciones

Objetivo	**Consulte**
Crear espacios de trabajo, situaciones y mandatos de Actualización personalizados.	• "Creación de espacios de trabajo, mandatos de Actuación y situaciones" en la página 1408
Empaquetar la extensión del soporte de aplicaciones.	• "Creación de extensiones de soporte de aplicaciones para agentes existentes" en la página 1512
Crear paquetes personalizados.	• "Creación de paquetes de archivos sin agente" en la página 1536

Orígenes de datos y conjuntos de datos

Un agente puede supervisar información de uno o varios orígenes de datos. Presenta la información a la infraestructura de supervisión como atributos, que se organizan en conjuntos de datos.

Al crear un agente, debe definirle un *origen de datos*. Puede añadir más orígenes de datos. El origen de datos define cómo el agente recopila la información de supervisión.

Puede utilizar Agent Builder para crear agentes que utilizan información de supervisión de orígenes de datos de los siguientes *proveedores de datos*:

- Disponibilidad de proceso y servicio
- Disponibilidad del sistema de red (mediante ping de ICMP)
- Códigos de retorno de mandatos
- Salida de script
- Registro de sucesos de Windows
- Windows Management Instrumentation (WMI)
- Windows Performance Monitor (Perfmon)
- Simple Network Management Protocol (SNMP)
- Sucesos de SNMP
- Disponibilidad y tiempo de respuesta de Hypertext Transfer Protocol (HTTP)
- SOAP u otro origen de datos HTTP
- Java Database Connectivity (JDBC)
- Interfaz de programación de aplicación (API) Java
- Java Management Extensions (JMX)
- Common Information Model (CIM)
- Archivos de registro
- Registros binarios de AIX
- Socket

También puede utilizar otras herramientas de desarrollo para crear aplicaciones de supervisión personalizadas que pasen información al agente mediante orígenes de datos de la API Java, el registro y la salida de script.

Al añadir un origen de datos, Agent Builder añade el *conjunto de datos* correspondiente al agente. El conjunto de datos organiza la información que se presenta al entorno de supervisión. En IBM Tivoli Monitoring, un conjunto de datos se conoce como un *grupo de atributos*.

Un conjunto de datos puede constar de varios *atributos*, que son valores que proporciona el origen de datos. Cada vez que el entorno de supervisión consulta el agente, capta valores de los orígenes de datos y a continuación los devuelve como atributos en conjuntos de datos.

Algunos orígenes de datos pueden devolver varias *filas* de valores de atributos en la misma consulta, por ejemplo, si el origen de datos supervisa varios servicios simultáneamente.

La mayoría de los orígenes de datos presentan información como un solo conjunto de datos. Según la configuración, los orígenes de datos SNMP y JMX pueden proporcionar distintos conjuntos de información. Al añadir un origen de datos SNMP o JMX, Agent Builder crea varios conjuntos de datos para dar cabida a esta información.

Puede editar los conjuntos de datos para filtrar los datos y crear atributos *derivados* adicionales, es decir, atributos calculados a partir de atributos existentes utilizando una fórmula. También puede unirse a conjuntos de datos, creando un nuevo conjunto de datos con información de dos o más conjuntos de datos. De esta forma, los usuarios pueden visualizar información combinada de distintos orígenes de datos.

En IBM Tivoli Monitoring, puede visualizar todo el contenido de los atributos. También puede crear espacios de trabajo que presentan información de todos los conjuntos de datos de agente en una vista personalizada. Puede utilizar IBM Tivoli Monitoring para crear situaciones que se desencadenan cuando algún atributo alcanza un valor determinado. Una situación puede emitir una alerta y llamar a un mandato del sistema.

En IBM Cloud Application Performance Management, debe definir un panel de instrumentos de *resumen* para el agente, seleccionando hasta cinco atributos que se visualizan en el panel de instrumentos. Puede definir un panel de instrumentos de *detalles* que muestra información de todos los conjuntos de datos como tablas. Puede crear umbrales que se desencadenan cuando alguno de los atributos alcanza un valor determinado; no es necesario añadir este atributo al panel de instrumentos. Un panel de instrumentos puede emitir alertas.

Supervisión de varios servidores o instancias de un servidor

Un agente puede supervisar varios servidores, incluidas varias instancias del mismo servidor. Hay dos formas de crear estos agentes: varias instancias de un agente y subnodos dentro de un agente.

Varias instancias son una manera estándar de supervisar servidores de aplicaciones que pueden tener una serie de instancias similares en el mismo host. Muchos agentes estándar en IBM Tivoli Monitoring e IBM Cloud Application Performance Management dan soporte a varias instancias.

Con *varias instancias* instala un agente en un host supervisado y a continuación configura una o varias instancias, estableciendo un nombre para cada una. Configure una instancia del agente para cada instancia del servidor que desee supervisar. Cada instancia es una copia idéntica individual del agente y se puede iniciar y detener por separado.

También puede definir uno o varios tipos de *subnodo* en un agente. Cada tipo debe corresponder a un tipo distinto de recurso que puede supervisar un agente. Un tipo de subnodo contiene orígenes de datos y conjuntos de datos; también puede definir orígenes de datos y conjuntos de datos a nivel de agente, fuera de cualquier subnodo. Al instalar el agente en un host, puede configurar el número necesario de subnodos de cada tipo; para cada tipo de subnodo, puede establecer el número de subnodos independientemente. Para IBM Cloud Application Performance Management, puede crear un panel de instrumentos para el agente y un panel de instrumentos individual para cada subnodo.

Los subnodos requieren distintos pasos de configuración en el host supervisado. Además, para reconfigurar, añadir o eliminar un subnodo, debe detener y reiniciar todo el agente; una instancia se puede reconfigurar, añadir o eliminar sin que otras instancias resulten afectadas. Sin embargo, los subnodos tienen algunas ventajas:

- Con los subnodos puede supervisar una gran cantidad de instancias de servidor consumiendo menos recursos. En líneas generales, el número de instancias de agente de un tipo específico soportado en un único sistema es 10. Sin embargo, un agente puede supervisar hasta 100 servidores locales o remotos mediante subnodos.

- Un agente puede incluir tipos de subnodo para unas pocas clases distintas de servidor. En el sistema supervisado, puede configurar cualquier número de subnodos de cada tipo. Puede utilizar esta característica para conservar aún más los recursos.
- Un agente con subnodos puede proporcionar datos de todo el sistema a nivel de agente.

Se pueden definir varias instancias y subnodos para el mismo agente. En este caso, cada instancia puede incluir varios subnodos. Puede detener y reiniciar cada instancia independientemente de otras instancias; todos los subnodos de una instancia se detienen y reinician juntos.

Prueba, instalación y configuración de un agente

Puede crear un paquete de instalación para un agente y a continuación instalarlo en diversos hosts supervisados. Para algunos orígenes de datos, es necesario establecer valores de configuración para recopilar datos.

Una vez que se han definido los orígenes de datos y los atributos de un agente, puede probarlo ejecutándolo en Agent Builder. Puede probar un único conjunto de datos (grupo de atributos) o todo el agente.

Para probar el agente con más detalle y utilizarlo, puede crear una imagen de instalación. Esta imagen proporciona scripts para instalar y configurar el agente en cualquier agente supervisado.

Consejo: Antes de instalar el agente, asegúrese de que el agente de sistema operativo del entorno de supervisión (IBM Tivoli Monitoring o IBM Cloud Application Performance Management) esté instalado en el host.

Tras instalar el agente, es posible que deba configurarlo. Si el agente soporta varias instancias, debe configurar el agente para crear al menos una instancia.

Algunos orígenes de datos requieren valores de configuración adicionales; por ejemplo, para el origen de datos SNMP debe configurar la dirección IP del host que supervisa utilizando el protocolo SNMP. Utilice el script de configuración, que despliega el paquete de instalación, para establecer estos valores.

Como alternativa, puede establecer estos valores en Agent Builder antes de crear la imagen de instalación. En este caso no es necesario establecerlos de nuevo en los hosts supervisados.

Consejo: Es posible que los archivos de ayuda para su agente personalizado no se visualicen en Contenido de la ayuda después de actualizar servidor de Cloud APM. Para visualizar los archivos de ayuda, siga estos pasos:

1. Descargue la versión más reciente de IBM Agent Builder desde la suscripción de Cloud APM en IBM Marketplace.
2. Vuelva a crear el agente personalizado. Asegúrese de asignar un número de versión, fixpack, o nivel de parche superior en la página Información del agente.
3. Instale el agente personalizado en el host supervisado.
4. En la Consola de Cloud APM, pulse **Ayuda** > **Contenido de la ayuda** en la barra de navegación. Se visualizará la ayuda del agente personalizado.

Requisitos de sistema operativo

Los agentes creados por Agent Builder están soportados en varios sistemas operativos, en función del entorno de supervisión y de los valores que se han seleccionado al crear el agente.

En un entorno de Tivoli Monitoring, los agentes creados por Agent Builder pueden dar soporte a los siguientes sistemas operativos:

- AIX
- HP-UX
- Linux
- Solaris
- Windows

Los agentes dan soporte a las mismas versiones de sistema operativo que los agentes de sistema operativo. Para conocer los detalles, acceda al sitio web de Informes de compatibilidad de productos de software. Busque el nombre de producto `Tivioli Monitoring` y marque el recuadro de selección del componente `OS Agents & TEMA (Tivoli Enterprise Monitoring Agent)`.

En un entorno de IBM Cloud Application Performance Management, los agentes creados por Agent Builder pueden dar soporte a los siguientes sistemas operativos:

- AIX
- Linux
- Windows

Los agentes dan soporte a las mismas versiones que los agentes de sistema operativo. Para conocer los detalles, utilice los enlaces de la sección Component reports de System requirements (APM Developer Center).

Para ejecutar el agente de supervisión en un entorno de Tivoli Monitoring, instale el agente del sistema operativo adecuado en cada sistema supervisado donde se ejecuta el agente.

Para ejecutar el agente de supervisión en un entorno de IBM Cloud Application Performance Management, instale todos los agentes suministrados con IBM Cloud Application Performance Management en cada sistema supervisado donde se ejecuta el agente.

Nota: Los navegadores de Agent Builder funcionan en los orígenes de datos y la información accesible desde el sistema en el que se ejecuta Agent Builder. Asegúrese de ejecutar Agent Builder en uno de los tipos de sistemas siguientes:

- Un sistema que se ejecuta en el mismo nivel que el sistema operativo y las aplicaciones supervisadas para las que se está desarrollando el agente
- Un sistema que se conecta a otro sistema que se ejecuta en el mismo nivel que el sistema operativo y aplicaciones supervisadas para las cuales está desarrollando el agente

Características específicas de IBM Tivoli Monitoring

Agent Builder proporciona varias características que se aplican solo a to IBM Tivoli Monitoring.

Puede utilizar grupos de navegador para organizar los datos que visualiza el agente en los espacios de trabajo y las vistas de navegador de IBM Tivoli Monitoring. Un grupo de navegador combina los datos de varios grupos de atributos (conjuntos de datos) en una única vista, ocultando al usuario los conjuntos de datos individuales originales.

Puede utilizar Tivoli Enterprise Portal para crear espacios de trabajo, situaciones y mandatos de Actuación para el agente. A continuación, puede utilizar Agent Builder para guardar los espacios de trabajo, situaciones y mandatos de Actuación como archivos de soporte de la aplicación y empaquetarlos con el agente. Además, Agent Builder también puede importar espacios de trabajo, situaciones y mandatos de Actuación para otros agentes y crear archivos de soporte de aplicación personalizados para ellos.

Agent Builder puede generar un modelo de datos de Cognos para cada agente. Utilice el modelo de datos para importar la información del agente en Cognos Framework Manager, un componente de IBM Tivoli Common Reporting, para la creación de informes.

Instalación e inicio de Agent Builder

Antes de instalar IBM Agent Builder, asegúrese de que el sistema cumple los requisitos previos. A continuación, utilice el asistente de instalación o el procedimiento de instalación silenciosa para instalar Agent Builder.

Consejo: Para obtener información acerca de cómo instalar o modificar un *agente*, consulte “Instalación de un agente” en la página 1426.

Requisitos previos para instalar y ejecutar Agent Builder

Para instalar y ejecutar el Agent Builder, el sistema deberá cumplir determinados requisitos.

Para instalar Agent Builder, asegúrese de que dispone de lo siguiente:

- Un sistema con un mínimo de 1 GB de espacio libre de disco. Los agentes que desarrolle requerirán espacio de disco adicional.
- Un sistema operativo soportado. Agent Builder puede ejecutarse en los siguientes sistemas operativos:
  - Windows Windows
  - Linux Linux (solo x86 de 64 bits)
- Linux Si utiliza el sistema operativo Linux, debe instalar la biblioteca `libstdc++.so.`**5**. Puede instalar los paquetes siguientes que proporcionan esta biblioteca:
  - En Red Hat Enterprise Linux, `compat-libstdc++-33`
  - En SUSE Enterprise Linux, `libstdc++-33`

Windows En un sistema Windows, debe poder ejecutar Agent Builder como un usuario con permisos de administrador. Estos permisos garantizan que Agent Builder tiene un entorno coherente con los agentes que se han desarrollado con el mismo.

Linux En un sistema Linux puede ejecutar Agent Builder como usuario root o como un usuario normal. Sin embargo, si lo ejecuta como un usuario normal, la prueba de agentes estará limitada y, en algunos casos, es posible que no está disponible.

Requisitos detallados del sistema para Agent Builder

Utilice los Informes de compatibilidad de productos de software para ver los requisitos detallados del sistema para Agent Builder.

Acceda al sitio web de Informes de compatibilidad de productos de software. Busque el nombre de producto `IBM Agent Builder`.

Instalación de Agent Builder

Puede utilizar el asistente de instalación o el procedimiento de instalación silenciosa para instalar Agent Builder.

Consejo: Antes de instalar Agent Builder, desinstale las versiones anteriores. Para obtener más información sobre la desinstalación, consulte “Desinstalación de Agent Builder” en la página 1204. No se pierde información del agente existente cuando desinstala.

Utilización del asistente de instalación para instalar Agent Builder

Puede utilizar el asistente de instalación para instalar IBM Agent Builder.

Antes de empezar

Asegúrese de que el sistema cumple los requisitos previos. Para obtener información sobre los requisitos previos, consulte “Requisitos previos para instalar y ejecutar Agent Builder” en la página 1201.

Procedimiento

1. Si no se ha registrado en IBM Marketplace, regístrese con su IBMid y contraseña y vaya a **Productos y servicios**.

   La página **Productos y servicios** está disponible para los suscriptores activos. Si tiene algún problema, vaya al Foro de Cloud Application Performance Management o al Soporte de Marketplace.
2. Descargue el archivo de archivado de instalación de Agent Builder:
   a) En el recuadro de suscripción de Cloud APM, pulse **Gestionar** > **Descargas**.
   b) Seleccione **Multiplataforma** como sistema operativo.
   c) Seleccione el paquete IBM Agent Builder .

d) Pulse **Descargar** y guarde `IBM_Agent_Builder_Install.tar` en el sistema.

3. Extraiga el archivo de archivado de instalación.
4. Utilice el mandato siguiente en el directorio de la imagen extraída para iniciar la instalación:
   - Windows `setup.bat`
   - Linux AIX `./setup.sh`

   Importante: Ejecute el programa de instalación con el mismo ID de usuario con el que piense ejecutar Agent Builder.
5. Cuando se abra la ventana de **IBM Agent Builder**, seleccione el idioma y pulse **Aceptar**.
6. En la página **Introducción**, pulse **Siguiente**.
7. En la página **Acuerdo de licencia de software**, pulse **Acepto los términos del acuerdo de licencia**, y pulse **Siguiente**.
8. En la página **Elegir carpeta de instalación**, pulse una de las siguientes opciones:
   - **Siguiente** para instalar Agent Builder en el directorio especificado en el campo **¿Dónde desea instalar?**.
   - **Restaurar carpeta predeterminada** para instalar Agent Builder en un directorio predeterminado.
   - **Elegir** para seleccionar un directorio diferente.

   Nota: El nombre de directorio que elija no debe contener los caracteres siguientes:

   !
   #
   %
   ;

   Si incluye alguno de estos caracteres, es posible que Agent Builder no se inicie.
9. En la página **Resumen previo a la instalación**, pulse **Instalar**.
10. En la página **Instalación de IBM Agent Builder**, espere a que se abra la página **Instalación completada** y, a continuación, pulse **Terminado**.

Resultados

Windows Después de instalar Agent Builder, se añade una opción al menú Inicio y se añade un icono de Agent Builder al escritorio. Los archivos de registro de instalación se encuentran en *dir_instalación* `\IBM_Agent_Builder_InstallLog.xml`.

Linux AIX Después de instalar Agent Builder, el archivo ejecutable de Agent Builder se denomina *Ubicación_instalación*`/agentbuilder`. Los archivos de registro de instalación se encuentran en *dir_instalación*`/IBM_Agent_Builder_InstallLog.xml`.

Instalación silenciosa

Agent Builder puede instalarse de forma silenciosa. Este método no requiere un entorno gráfico y se puede duplicar fácilmente en varios hosts.

Acerca de esta tarea

El archivo de opciones de la instalación silenciosa, `installer.properties`, se incluye en la imagen de instalación que hay en el directorio raíz de la instalación. Debe modificar este archivo para satisfacer sus necesidades y, a continuación, ejecutar el instalador de forma silenciosa. Puede copiar este archivo en otros hosts e instalar rápidamente Agent Builder en todos los demás.

Procedimiento

1. Si no se ha registrado en IBM Marketplace, regístrese con su IBMid y contraseña y vaya a **Productos y servicios**.

La página **Productos y servicios** está disponible para los suscriptores activos. Si tiene algún problema, vaya al Foro de Cloud Application Performance Management o al Soporte de Marketplace.

2. Descargue el archivo de archivado de instalación de Agent Builder:
   a) En el recuadro de suscripción de Cloud APM, pulse **Gestionar** > **Descargas**.
   b) Seleccione **Multiplataforma** como sistema operativo.
   c) Seleccione el paquete IBM Agent Builder .
   d) Pulse **Descargar** y guarde `IBM_Agent_Builder_Install.tar` en el sistema.
3. Extraiga el archivo de archivado de instalación.
4. Cree una copia del archivo `installer.properties`, que está ubicado en el directorio de la imagen de instalación.
5. Edite el nuevo archivo conforme a sus necesidades. Un ejemplo del contenido de dicho archivo sería:

```
# ------------------------------------------------------------------
# IBM Agent Builder
#
# (C) Copyright IBM Corporation 2009.  Reservados todos los derechos.
#
# Archivo de respuestas de ejemplo para la instalación silenciosa
#
# Para utilizar este archivo, ejecute el mandato siguiente:
#
# Windows:
#    setup.bat -i silent -f <vía_acceso>\installer.properties
#
# Linux o AIX:
#    setup.sh -i silent -f <vía_acceso>/installer.properties
#
# Donde
#    <vía_acceso> es una vía de acceso completa para el archivo de propiedades del
#    instalador (incluida la letra de unidad o el nombre de vía de acceso UNC en Windows).
#    El valor de <vía_acceso> no puede tener espacios.
# ------------------------------------------------------------------


# ------------------------------------------------------------------
# Esta propiedad indica que la licencia se ha aceptado
# ------------------------------------------------------------------
# LICENSE_ACCEPTED=FALSE

# ------------------------------------------------------------------
# Esta propiedad especifica el directorio de instalación
#
# En Windows, el valor predeterminado es:
#     C:\\Archivos de programa (x86)\\IBM\\AgentBuilder
#
# En Linux, el valor predeterminado es:
#     /opt/ibm/AgentBuilder
# ------------------------------------------------------------------
#USER_INSTALL_DIR=C:\\Archivos de programa (x86)\\IBM\\AgentBuilder
#USER_INSTALL_DIR=/opt/ibm/AgentBuilder
```

6. Inicie la instalación silenciosa ejecutando el siguiente comando en el directorio de la imagen de instalación:

   Windows `setup.bat -i silent -f` *vía_acceso*`/installer.properties`

   Linux AIX `./setup.sh -i silent -f` *vía_acceso*`/installer.properties`

   Donde *vía_acceso* es la vía de acceso completa al archivo `installer.properties` (incluida la letra de unidad o nombre de vía de acceso UNC en Windows). La vía de acceso no puede contener espacios.

Inicio de Agent Builder

Tras instalar Agent Builder, pude iniciarlo.

Procedimiento

- Inicie Agent Builder utilizando uno de los métodos siguientes

- Windows En sistemas Windows:
  - En la línea de mandatos, escriba: *Ubicación_instalación*\agentbuilder.exe.
  - Seleccione **Start** > **Todos los programas** > **IBM** > **Agent Builder**.
  - Pulse el **Icono de escritorio Agent Builder**.
- Linux En sistemas Linux, ejecute el siguiente archivo ejecutable: *DIR_INSTAL*/agentbuilder

Nota: Al ejecutar Agent Builder, este solicita la ubicación del directorio de espacio de trabajo. Los archivos que creen los agentes se guardarán en dicho directorio. Puede designar cualquier directorio como espacio de trabajo.

Establecimiento del navegador predeterminado en Agent Builder

Linux En sistemas Linux, es posible que tenga que establecer el navegador predeterminado de Agent Builder, de modo que se visualicen los paneles de ayuda.

Procedimiento

1. Seleccione **Ventana** > **Preferencias** para abrir la ventana **Preferencias**.
2. Seleccione y expanda el nodo **General**.
3. Seleccione **Navegador web**.
4. Seleccione **Utilizar navegador web externo**.
5. Seleccione el navegador que desea utilizar.
6. Opcional: Para añadir un navegador web, realice los pasos siguientes
   a) Pulse **Nuevo**.
   b) En el campo **Nombre**, especifique un nombre descriptivo para el navegador.
   c) En el campo **Ubicación**, especifique la vía de acceso completa al archivo ejecutable del navegador.
   d) Pulse **Aceptar**.
7. Pulse **Aceptar**.

Establecimiento de la Autoridad de indicación de fecha y hora predeterminada en Agent Builder

Puede establecer la Autoridad de indicación de fecha y hora para archivos JAR en la ventana **Preferencias** de Agent Builder. El el certificado de firma de Autoridad de indicación de fecha y hora caduca, puede establecer una autoridad nueva para seguir verificando archivos JAR.

Procedimiento

1. Seleccione **Ventana** > **Preferencias** para abrir la ventana **Preferencias**.
2. Seleccione y expanda el nodo **IBM Agent Builder**.
3. Seleccione **Firma de JAR**.
4. Seleccione **Añadir indicación de fecha y hora a archivos JAR firmados**.
5. Especifique el URL de la autoridad de indicación de fecha y hora.
6. Pulse **Aceptar**.

Desinstalación de Agent Builder

Dependiendo del sistema operativo, pueden seguirse distintos procedimientos de desinstalación de Agent Builder.

Procedimiento

- Linux

En sistemas Linux, ejecute el mandato siguiente:

a) *DIR_INSTALACIÓN*/uninstall/uninstaller

donde *DIR_INSTALACIÓN* es el nombre del directorio en el que está instalado Agent Builder.

- Windows

  En Windows 7, Windows Server 2008 R2 y versiones posteriores de Windows, siga los pasos siguientes:

  a) Abra Programas y características de Windows seleccionando **Inicio** > **Panel de control** > **Programas** > **Programas y características**.

  b) Seleccione **IBM Agent Builder** en la lista de programas instalados.

  c) Pulse **Desinstalar/Cambiar**.

  d) Pulse **Desinstalar** en la página **Desinstalar IBM Agent Builder**.

  e) Pulse **Terminado** en la página **Desinstalación completada**.

  Consejo: En Windows 7 y Windows Server 2008 R2, puede también ir a la ventana **Programas y características de Windows** si selecciona **Inicio** > **Sistema** > **Desinstalar o cambiar un programa**. Luego siga a partir del paso "2" en la página 1205.

- Windows

  En otros sistemas Windows, siga los pasos siguientes:

  a) En el Panel de control de Windows, seleccione **Agregar o quitar programas**.

  b) Pulse **IBM Agent Builder**.

  c) Pulse **Cambiar o quitar**.

- En todos los sistemas operativos también se puede aplicar el método de desinstalación silenciosa. Inicie la desinstalación silenciosa ejecutando el siguiente mandato:

  - Windows En sistemas Windows, *DIR_INSTALACIÓN*/uninstall/uninstaller.exe -i silent
  - Linux En sistemas Linux, *DIR_INSTALACIÓN*/uninstall/uninstaller -i silent

Desinstalación silenciosa

Puede utilizar el método de desinstalación silenciosa para desinstalar.

Procedimiento

- Inicie la desinstalación silenciosa ejecutando el siguiente mandato:

```
INSTALL_DIR/uninstall/uninstaller[.exe] -i silent
```

Crear un agente

Para empezar a crear un agente en Agent Builder, utilice el asistente de agente nuevo. Con este asistente puede establecer la configuración de agente básico y crear el origen de datos. A continuación, puede trabajar en el agente en Agent Builder para añadir más orígenes de datos y otras opciones, incluidos subnodos y grupos de navegador.

Denominación y configuración del agente

Utilice el **Asistente de agente** para poner nombre al agente, establecer la versión, los sistemas operativos admitidos y otros valores de configuración.

Procedimiento

1. Utilice una de las siguientes formas para iniciar el nuevo asistente de agente:

a) Pulse el icono **Crear nuevo agente** en la barra de herramientas.

b) En el menú principal, seleccione **Archivo** > **Nuevo** > **Agente**.

c) En el menú principal, seleccione **Archivo** > **Nuevo** > **Otro**. En la página **Seleccionar un asistente**, efectúe una doble pulsación en la carpeta **Agent Builder**. luego efectúe una doble pulsación en **Agente**.

Se abrirá el **Asistente de agente**.

2. Pulse **Siguiente**.
3. En la página **Proyecto de agente nuevo**, establezca el nombre del proyecto en el campo **Nombre de proyecto**. Agent Builder utiliza este nombre para la carpeta que contiene los archivos del agente. Opcionalmente, puede cambiar los valores siguientes:
   - Si desea almacenar los archivos del agente en otra ubicación, deseleccione **Utilizar la ubicación predeterminada** y pulse **Examinar** para seleccionar el nuevo directorio en el campo **Ubicación**.
   - Puede cambiar la forma en que la vista de Navigator de Eclipse muestra recursos añadiéndolos a varios conjuntos de trabajo. Para obtener más información, consulte la ayuda de Eclipse. Para añadir el agente a los conjuntos de trabajo de Eclipse, seleccione **Añadir proyecto a conjuntos de trabajo** y pulse el botón **Seleccionar** para añadir los conjuntos al campo **Conjuntos de trabajo**.
4. Pulse **Siguiente**.
5. En la página **Información general**, configure los valores siguientes:
   - Escriba la declaración de copyright que desea utilizar para los agentes nuevos en el campo **Copyright**. Esta declaración debe adaptarse a los requisitos legales de copyright. Esta declaración de copyright se inserta en todos los archivos que se generan para el agente y se puede editar posteriormente.
   - Seleccione los sistemas operativos para los que desee crear el agente.

     Importante: Si desea ejecutar una prueba completa del agente dentro de Agent Builder (consulte "Prueba de todo el agente" en la página 1421 para obtener las instrucciones), asegúrese de que:

     – Si está ejecutando Agent Builder en Windows, esté instalada la versión de 32 bits del sistema operativo.

     – Si está ejecutando Agent Builder en Linux, esté instalada la versión de 64 bits del sistema operativo.

     Importante: En algunos casos excepcionales, es posible que tenga que instalar el agente en un sistema de 64-bits donde solo está instalado el agente del sistema operativo de 32-bits. En este caso, asegúrese de que la versión de 64 bits del sistema operativo no está seleccionada y que está seleccionada la versión de 32 bits.

     Importante: los agentes creados mediante Agent Builder no admiten Windows Server 2003 R2 de 64 bits y sistemas Windows anteriores.
6. Pulse **Siguiente**.
7. En la página **Información de agente**, configure los valores siguientes:
   - Establezca el nombre de servicio del agente en el campo **Nombre de servicio**. El nombre que se visualiza en la ventana **Manage Tivoli Monitoring Services** en un entorno IBM Tivoli Monitoring y en el programa de utilidad **Gestionar servicios de supervisión** y el Editor de umbrales en IBM Cloud Application Performance Management. En sistemas Windows, también es el nombre del servicio Windows que ejecuta el agente. El nombre de servicio completo siempre empieza con `Monitoring Agent for`. Puede especificar la parte restante del nombre que normalmente describe el servicio que este agente supervisa. El nombre puede contener letras, números, espacios y signos de subrayado.
   - Establezca un código de producto de tres caracteres para el agente en el campo **Código de producto**. Se requiere un nombre de producto para IBM Tivoli Monitoring e IBM Cloud Application

Performance Management. Hay un rango de códigos de producto reservados para utilizarlos con Agent Builder. Los valores permitidos son `K00-K99`, `K{0-2}{A-Z}` y `K{4-9}{A-Z}`.

Importante: Estos valores son solo para uso interno y no están destinados a agentes que se vayan a compartir o vender fuera de la organización. Si está creando un agente para compartirlo con otras personas, deberá enviar una nota a toolkit@us.ibm.com para reservar un código de producto. La solicitud de un código de producto debe incluir una descripción del agente que se va a crear. A continuación se asigna, registra y se le devuelve un código de producto. Cuando recibe el código de tres dígitos del producto, se le indica cómo habilitar Agent Builder para utilizar el código de producto asignado.

- Establezca una serie que identifique de forma exclusiva a la organización que desarrolla el agente en el campo **Identificador de compañía** (`IBM` está reservado). Puede tomar este nombre del URL de la empresa; por ejemplo, si el sitio web de la empresa es `miempresa.com`, utilice el texto `miempresa`.
- Establezca una serie que identifique de forma exclusiva al agente en el campo **Identificador de agente**. De forma predeterminada, Agent Builder establece el identificador del agente en el valor del código de producto.

  Importante: La longitud combinada del campo **Identificador de agente** y el campo **Identificador de compañía** no puede superar los 11 caracteres.
- Establezca la versión del agente en el campo **Versión**. La versión del agente contiene tres dígitos con el formato *V.R.R*, donde:

  V = Versión
  R = Release
  R = Release

  Para su visualización en el entorno de supervisión, el valor *V.R.R* se convierte al formato siguiente: `0V.RR.00.00`

  Consejo: En el editor de agente, un campo **nivel de parche** está disponible. El campo **nivel de parche** puede utilizarse cuando publique un arreglo para un agente, sin actualizar la versión.
- Si desea que el agente admita varias instancias, seleccione el recuadro de selección **Soportar varias instancias de este agente**. Puede utilizar varias instancias de un agente para supervisar varias instancias de una aplicación en el mismo host, o utilizar un agente instalado en un único host para supervisar varios servidores de software en distintos hosts. Cuando instala un agente que da soporte a varias instancias, puede crear y configurar tantas instancias como se requiera.

Qué hacer a continuación
Pulse **Siguiente** para definir un origen de datos inicial para el agente. Para obtener más información, consulte “Definición de orígenes de datos iniciales” en la página 1207

Definición de orígenes de datos iniciales

Al crear un agente, defina los datos iniciales que va a supervisar el agente. Puede añadir más orígenes de datos posteriormente en el editor del agente.

Acerca de esta tarea
Defina los orígenes de datos que el nuevo agente debe supervisar utilizando la página **Origen de datos inicial de agente**. Para obtener las instrucciones detalladas de creación de orígenes de datos de varios proveedores de datos, consulte “Definición y prueba de orígenes de datos” en la página 1256.

Procedimiento

1. En la página **Origen de datos inicial de agente**, seleccione una de las **Categorías de datos de supervisión** y uno de los **Orígenes de datos**.
2. Pulse **Siguiente**. El asistente le guía por el proceso de definir y configurar los tipos de recopilación de datos que especifique.

Consejo: Puede utilizar este asistente para definir un origen de datos o añadir un subnodo o grupo de navegador para organizar el agente. Para obtener más información sobre los subnodos, consulte “Utilización de subnodos” en la página 1384. Para obtener más información sobre los grupos de navegador, que se utilizan solo para IBM Tivoli Monitoring, consulte “Creación de un grupo de Navigator” en la página 1383.

3. Si ha definido un nuevo origen de datos que puede que devuelva más de una fila de datos, se le solicitará que seleccione atributos clave. Para obtener más información, consulte (“Selección de atributos clave” en la página 1208).
4. Una vez que se ha definido el primer origen de datos, se visualiza la ventana **Definición de origen de datos**. Para añadir otro origen de datos, seleccione el agente, o un subnodo o grupo de navegador si hay uno presente, y pulse el botón **Añadir a seleccionados**.
5. Para acabar de definir los orígenes de datos, pulse **Finalizar**. Agent Builder crea el nuevo agente y lo abre en el editor del agente.

Selección de atributos clave
Cuando un grupo de atributos devuelve más de una fila de datos, debe seleccionar atributos clave.

Acerca de esta tarea

Cuando un grupo de atributos puede devolver más de una fila de datos, cada fila representa una entidad que se supervisa. Cada vez que se muestrean datos supervisados, el entorno de supervisión compara una fila con la entidad que se está supervisando y con muestras anteriores para dicha entidad. Esta comparación se hace con atributos clave. Uno o varios atributos del grupo de atributos se pueden identificar como atributos clave. Estos atributos clave, tomados en conjunto, distinguen una entidad supervisada de otra. Los atributos clave no cambian de una muestra a otra para la misma entidad supervisada.

Los atributos de tasa y delta se calculan comparando la muestra actual con la muestra anterior. Atributos clave idénticos aseguran que el agente compara valores para la misma entidad supervisada. De forma similar, el agente de resumen y poda resume muestran que tienen atributos clave idénticos. Además, cualquier atributo que se establezca como un atributo clave también se puede utilizar como un "Elemento de visualización" en una situación.

Los detalles del nuevo origen de datos se especifican en la página **Origen de datos inicial del agente**. Cuando el origen de datos seleccionado devuelve varias filas de datos, a veces Agent Builder puede detectar los atributos clave. En caso contrario, le solicitará que seleccione dichos atributos clave.

Procedimiento

- En la página **Seleccionar atributos clave**, siga uno de estos pasos:
  - Pulse uno o varios atributos de la lista que sean atributos clave para esta entidad. Para seleccionar más de un atributo, mantenga pulsada la tecla Ctrl.
  - Si este grupo de atributos devuelve solo una fila, seleccione **Produce una sola fila de datos**. Si se selecciona esta opción, no se necesita ningún atributo clave porque solo se notifica una entidad supervisada en este grupo de atributos.

Utilización del editor del agente para modificar el agente

Utilice el editor del agente para cambiar, guardar y confirmar una versión del agente.

Puede crear un agente nuevo en el Agent Builder; si desea más información, consulte “Crear un agente” en la página 1205. Tras crear un agente, puede modificarlo utilizando el editor del agente.

Para abrir un agente que haya creado en Agent Builder en el editor del agente, en el panel **Explorador de proyectos** busque el nombre del agente y expándalo. En el nombre del agente, efectúe una doble pulsación en **Definición de agente**. Como alternativa, efectúe una doble pulsación en el nombre de archivo `itm_toolkit_agent.xml`.

El editor del agente es un editor Eclipse de varias páginas que puede utilizar para modificar las propiedades de un agente existente. Cada página del editor corresponde a una función específica del agente.

La lista de páginas disponibles se muestra en la vista esquema debajo del nodo de **Definición de agente**. Puede cambiar con facilidad a otra página pulsando en un nodo de la vista Esquema. Si falta la vista de esquema, o está oculta detrás de otra vista, puede restablecer la perspectiva de la definición del agente. Restaure la perspectiva seleccionando **Ventana** > **Restaurar perspectiva**. De forma alternativa, pulse el botón derecho del ratón en la pestaña **Definición de agente** y seleccione **Restablecer** en el menú.

Nota: Para obtener información detallada y procedimientos para crear un agente, consulte "Crear un agente" en la página 1205.

En Agent Editor se incluyen las páginas siguientes:

- "Página Información de agente" en la página 1209
- Página Definición de origen de datos
- Página Información de configuración de tiempo de ejecución
- Página XML de agente del editor (itm_toolkit_agent.xml)

Nota: Cuando visualiza una página Editor, puede también conmutar a otra página pulsando la pestaña de la página. Algunas páginas muestran pestañas únicamente cuando están seleccionadas en la Vista de esquema. Puede forzar a que una página tenga una pestaña incluso cuando no se haya seleccionado. Para forzar a que una página tenga una pestaña, pulse el icono de fijación de modo que la fijación del icono apunte hacia la página.

Página Información de agente

La página **Información de agente** es la página principal del Agent Editor.

La página **Información de agente** contiene la siguiente información:

- Información general de agente, incluidos el nombre de servicio y el código de producto. Puede pulsar **Avanzado** para establecer nombres diferentes para usos diferentes, pero normalmente este valor no es necesario.
- Información Contenido de agente
  - Enlace **Sistemas operativos predeterminados**
  - Enlace **Agente de autodescripción**
  - Enlace **Variables de entorno**
  - Enlace **Información sobre proceso de vigilancia**
  - Enlace **Información de Cognos**
  - Enlace **Orígenes de datos**
  - Enlace **Configuración de tiempo de ejecución**
  - Enlace **Recursos**
  - Enlace **Paneles de instrumentos**
- Enlace **Probar agente**
- Enlace **Asistente para generar agente**
- Enlace **Confirmar versión de agente**

Configuración del tiempo para los mensajes de error transitorios

El asistente de Agent Editor a veces visualiza mensajes de error transitorios. Se visualiza un mensaje durante un período de tiempo corto (por omisión, 3 segundos) en la cabecera del asistente. Puede configurar la duración durante la que se visualizan estos mensajes. Para cambiar este valor:

1. Seleccione **Ventana** > **Preferencias** en la barra de menús de Agent Builder. Se abrirá la ventana **Preferencias**.

2. Seleccione **Agent Builder**.
3. Establezca el valor de **Tiempo (en segundos) que se visualiza el mensaje de error transitorio**.
4. Pulse **Aceptar**.

Sistemas operativos predeterminados

Utilice la página **Sistemas operativos predeterminados** para cambiar los sistemas operativos para los que se crea el agente.

Procedimiento

- Para abrir la página **Sistemas operativos predeterminados**, pulse **Sistemas operativos predeterminados** en la sección **Contenido de agente** de la página **Información de agente** o el nodo **Sistemas operativos predeterminados** en la Vista de esquema.
- En la página **Sistemas operativos predeterminados**, seleccione los sistemas operativos que tiene que soportar el agente.

  Cuando se genera un paquete de instalación para el agente, Agent Builder añade a dicho paquete los archivos de los sistemas operativos seleccionados. Los orígenes de datos que añade al agente que no son específicos del sistema operativo Windows están disponibles en cualquiera de los sistemas operativos seleccionados. Los sistemas operativos en los que cualquier origen de datos específico está disponible se pueden cambiar en esta selección predeterminada. Para cambiar los sistemas operativos disponibles para un origen de datos específico, utilice el panel **Sistemas operativos** de la página **Definición de origen de datos**. Si no se seleccionan sistemas operativos predeterminados, se deben seleccionar para cada origen de datos específico en la página **Definición de origen de datos**.

  Importante: Si desea ejecutar una prueba completa del agente dentro de Agent Builder (consulte "Prueba de todo el agente" en la página 1421 para obtener las instrucciones), asegúrese de que:

  – Si está ejecutando Agent Builder en Windows, esté instalada la versión de 32 bits del sistema operativo.
  – Si está ejecutando Agent Builder en Linux, esté instalada la versión de 64 bits del sistema operativo.

  Importante: En algunos casos excepcionales, es posible que tenga que instalar el agente en un sistema de 64-bits donde solo está instalado el agente del sistema operativo de 32-bits. En este caso, asegúrese de que la versión de 64-bits del sistema operativo no está seleccionada y que está seleccionada la versión de 32-bits.

Agente de autodescripción

Para el entorno de IBM Tivoli Monitoring, utilice la página **Agente de autodescripción** para especificar si los archivos de soporte del agente están empaquetados con el agente. En el caso del entorno de IBM Cloud Application Performance Management, hay que dejar habilitado el agente de autodescripción.

Procedimiento

- Para abrir la página **Agente de autodescripción**, pulse **Agente de autodescripción** en la sección **Contenido de agente** de la página **Información de agente** o el nodo **Agente de autodescripción** en la vista Esquema.

  La autodescripción está habilitada de forma predeterminada para todos los agentes nuevos que se crean con Agent Builder 6.2.3 o posterior. Si el agente es para el entorno de IBM Cloud Application Performance Management, deberá estar habilitada la autodescripción.

  Cuando la autodescripción se habilita para un agente, los paquetes de soporte de aplicaciones se incluyen en la imagen del agente. Esta inclusión permite que el agente inicie los archivos de soporte para Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, Tivoli Enterprise Portal Browser. Para obtener más información acerca de los agentes de autodescripción, consulte las publicaciones *IBM Tivoli Monitoring: Guía de instalación y configuración* e *IBM Tivoli Monitoring: Guía del administrador*. En un entorno IBM Cloud Application Performance Management, la autodescripción

permite al agente iniciar archivos de soporte en el Servidor de Cloud APM; la inicialización es un paso necesario en el entorno.

Nota: En un entorno IBM Tivoli Monitoring, debe tener Tivoli Monitoring versión 6.2.3 o posterior instalado para que funcione la característica del agente de autodescripción, y la autodescripción debe estar habilitada en Tivoli Monitoring. De forma predeterminada, la autodescripción está desactivada en Tivoli Monitoring.

Nota: La selección del recuadro de selección **Habilitar la autodescripción para este agente** no impedirá al agente trabajar sobre versiones anteriores de Tivoli Monitoring.

Variables de entorno

Utilice la página **Variables de entorno** para ver y modificar variables de entorno que están disponibles para el agente mientras se ejecuta.

Antes de empezar

Para obtener más información sobre **Agent Editor** y la página **Información de agente**, consulte "Utilización del editor del agente para modificar el agente" en la página 1208.

Acerca de esta tarea

Las variables de entorno pueden ser definidas por el usuario, para acceder dentro de un script, o variables predefinidas que hacen que el agente se comporte de una forma determinada. Consulte la "Lista de variables de entorno" en la página 1211 para obtener una lista de variables predefinidas.

Procedimiento

1. Para abrir la ventana **Variables de entorno**, pulse **Variables de entorno** en la sección **Contenido de agente** de la página **Información de agente**. De forma alternativa, pulse el nodo **Variables de entorno** en la vista **Esquema**.
2. En la página **Variables de entorno**, pulse **Añadir** para añadir una nueva variable. De forma alternativa, para editar una variable existente, selecciónela y pulse **Editar**.
3. En la ventana **Información sobre variables de entorno**, establezca los siguientes valores:
   - En el campo **Nombre**, escriba un nombre de variable o seleccione un nombre predefinido en la lista.
   - En el campo **Valor**, escriba un valor para la variable si desea establecer una variable para el agente. Si no especifica ningún valor, el agente propagará un valor para la variable existente.
   - En el campo **Descripción**, escriba una descripción de la variable, o guarde la descripción existente de una variable predefinida.

   a) Pulse **Aceptar**.

   La nueva variable aparece en la tabla de la página **Información de agente**.

Lista de variables de entorno

Utilice las variables de entorno para controlar el comportamiento del agente en tiempo de ejecución.

Las variables de entorno pueden crearse en el agente mediante la página **Variables de entorno**. En los sistemas Windows, las variables de entorno se definen en el archivo K*XX*ENV del agente. En los sistemas UNIX y Linux, estas variables se pueden definir en el archivo `$CANDLEHOME/config/XX.ini` del agente. *XX* es el código de producto de dos letras. Para que los valores nuevos tengan efecto, el agente se debe reiniciar.

Nota: Las variables de entorno no se han establecido correctamente en un sistema remoto que ejecuta C Shell. Utilice un shell distinto si desea utilizar las variables de entorno.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_*GRUPO_ATRIBUTOS*_REFRESH_INTERVAL	No aplicable	Un entero no negativo	Intervalo en segundos durante el cual un grupo de atributos especificado concreto se actualiza en segundo plano. Esta variable funciona del mismo modo que CDP_DP_REFRESH_INTERVAL, excepto en que tiene como destino únicamente el grupo de atributos especificado. El nombre de grupo de atributos del nombre de variable debe estar en mayúsculas, aunque el nombre de grupo de atributos real no esté en mayúsculas.
CDP_DP_CACHE_TTL	55	Un entero superior o igual a 1.	Los datos se recopilan para un grupo de atributos almacenados en la memoria caché por este número de segundos. Cuando se realizan varias solicitudes de los mismos datos en este intervalo de tiempo, éstas reciben una copia de los datos almacenada en la memoria caché. Este valor se aplica a todos los grupos de atributos del agente.
CDP_*GRUPO_ATRIBUTOS*_CACHE_TTL	Valor de CDP_DP_CACHE_TTL	Un entero superior o igual a 1.	Los datos que se recopilan para el grupo de atributos especificado se almacenan en la memoria caché durante este número de segundos. Cuando se realizan varias solicitudes de los mismos datos en este intervalo de tiempo, éstas reciben una copia de los datos almacenada en la memoria caché. Este valor altera temporalmente CDP_DP_CACHE_TTL para el grupo especificado. El nombre de grupo de atributos del nombre de variable debe estar en mayúsculas, aunque el nombre de grupo de atributos real no esté en mayúsculas.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT	5 si se definen subnodos, de lo contrario no se establece	Un entero positivo	El número de segundos a esperar por una recopilación de datos antes de un tiempo de espera excedido y la devolución de los datos almacenados en caché, incluso si los datos de caché son obsoletos. (Los datos de la memoria caché están obsoletos si son anteriores a CDP_DP_CACHE_TTL segundos). Si esta variable no se establece, el agente espera hasta que la recopilación de datos se completa. A veces la espera puede hacer que Tivoli Enterprise Portal exceda el tiempo de espera y deje de esperar. Si no hay ninguna agrupación de hebras configurada, esta variable se ignora y la recopilación de datos se realiza de forma síncrona.
CDP_DP_REFRESH_INTERVAL	60 si se definen subnodos, de lo contrario no se establece	Un entero no negativo	Intervalo en segundos durante el cual se actualizan en segundo plano grupos de atributos. Si esta variable no se establece o se establece en 0, las actualizaciones en segundo plano se inhabilitan. Si está configurada una agrupación de hebras (consulte la variable CDP_DP_THREAD_POOL_SIZE), los grupos de atributos se renuevan en paralelo. Si no existe ninguna agrupación de hebras, las actualizaciones se producirán en serie y pueden tardar más bastante tiempo. Es lógicamente equivalente a un tamaño de agrupación de hebras de 1.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_DP_THREAD_POOL_SIZE	15 si hay subnodos definidos, de lo contrario no se establece	Un entero no negativo	El número de hebras que se crean para ejecutar las colecciones de datos en segundo plano en un intervalo que define CDP_DP_REFRESH_INTERVAL. Si esta variable no se establece o se establece en 0, no existe ninguna agrupación de hebras. Si CDP_DP_THREAD_POOL_SIZE se establece en un valor mayor que 1 y CDP_DP_REFRESH_INTERVAL se establece en 0, el valor de CDP_DP_THREAD_POOL_SIZE se ignora y la recopilación de datos se realiza a petición. El grupo de atributos Estatus de agrupación de hebras muestra cómo se ejecuta la agrupación de hebras. Utilice Estatus de agrupación de hebras para ajustar el tamaño de la agrupación de hebras y el intervalo de renovación para obtener los mejores resultados. De forma predeterminada, la consulta para este grupo de atributos no se visualiza en el árbol de Navigator de agente. Es posible que no recuerde que debe incluir la consulta en un espacio de trabajo personalizado para el agente. Sin embargo, puede verlo fácilmente asignando la consulta Estatus de agrupación de hebras a una vista del espacio de trabajo de nivel de agente básico.
CDP_JDBC_MAX_ROWS	1000	Un entero positivo	El número máximo de filas de datos que devuelve el proveedor de datos JDBC. Un conjunto de resultados que contiene más de este número de filas solo se procesa hasta este valor máximo. Se pueden desarrollar consultar para evitar que se devuelvan demasiados datos a IBM Tivoli Monitoring.
CDP_NT_EVENT_LOG_GET_ALL_ENTRIES_FIRST_TIME	NO	YES, NO	Si se establece YES como valor, el agente enviará un suceso para por cada suceso del registro de sucesos de Windows. Si se establece NO como valor, sólo se enviarán los sucesos nuevos del registro de sucesos de Windows.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_NT_EVENT_LOG_CACHE_TIMEOUT	3600	Un entero superior o igual a 300.	Número de segundos durante los cuales el agente almacena en la memoria caché los sucesos del registro de sucesos de Windows. Todos los sucesos almacenados en la memoria caché se devuelven cuando se consulta el grupo de atributos de registro cronológico de sucesos. **Nota:** Esta variable ya no se utiliza. Utilice la variable CDP_PURE_EVENT_CACHE_SIZE.
CDP_PURE_EVENT_CACHE_SIZE	100	Un entero positivo superior o igual a 1	Número máximo de sucesos a almacenar en la memoria caché de un archivo de registro que se configura para procesar nuevos registros, para el grupo de atributos de Windows Event Log. Y también para notificaciones y supervisores de JMX. Cada nuevo registro del registro hará que se envíe un suceso. Esta variable de entorno define cuántos sucesos recuerda el agente en una memoria caché. Los valores almacenados en la memoria caché se devuelven cuando se consulta el grupo de atributos.
CDP_DP_ACTION_TIMEOUT	20 segundos	Un entero positivo superior o igual a 1	El número de segundos que se debe esperar para que se complete una actuación que el agente está manejando.
CDP_DP_SCRIPT_TIMEOUT	30 segundos	Un entero positivo superior o igual a 10	El número de segundos que se debe esperar a que el programa iniciado por un grupo de atributos basado en script se complete.
CDP_DP_PING_TIMEOUT	30 segundos	Un entero positivo superior o igual a 10	El número de segundos que se debe esperar a que el programa iniciado por un código de retorno de mandato se complete. **Nota:** Esta variable no está relacionada con el proveedor de datos de ping de ICMP.
CDP_SNMP_MAX_RETRIES	2	Un entero positivo	El número de veces que se debe intentar enviar la solicitud de SNMP de nuevo. El número total de solicitudes que se envían al agente SNMP es este valor más uno si no se reciben respuestas.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_SNMP_RESPONSE_TIMEOUT	2 segundos	Un entero positivo	El número de segundos a esperar para que cada solicitud de SNMP alcance el tiempo de espera excedido. Cada fila de un grupo de atributos es una solicitud independiente. Este valor de tiempo de espera es el número de segundos que se debe esperar una respuesta antes de intentarlo nuevamente. El tiempo de espera total para una única fila de datos es (CDP_SNMP_MAX_RETRIES + 1) * CDP_SNMP_RESPONSE_TIMEOUT. El valor total predeterminado de tiempo de espera es (2+1) * 2 = 6 segundos.
CDP_DP_HOSTNAME	Nombre de la primera interfaz de red instalada	Una dirección IP o nombre de host	Establece el nombre de host preferido (interfaz de red) en un sistema de varias interfaces. Utilice esta variable de entorno si el agente enlaza sus puertos de escucha a una dirección de interfaz de red que no sea la predeterminada. Se utiliza por el proveedor de datos SNMP. Para los orígenes de datos de socket, esta variable se aplica si CDP_DP_ALLOW_REMOTE también se ha establecido.
CDP_SNMP_ALLOW_ DECREASING_OIDS	NO	YES, NO	Si tiene el valor YES, los proveedores de datos SNMP no comprueban si los IOD devueltos son ascendentes. Establezca el valor YES con precaución ya que el agente supervisado puede tener problemas que normalmente esta comprobación detectaría.
KUMP_DP_COPY_MODE_SAMPLE_INTERVAL	60	Tiempo de espera en segundos	Para un proveedor de datos de archivo de registro, especifica cuánto tiempo se debe esperar antes de volver a leer el contenido de un archivo cuando el agente está definido para **Procesar todos los registros cuando se muestra el archivo**. El tiempo se especifica en segundos.
KUMP_MAXPROCESS	100%	5-100%	Para un proveedor de datos de archivo de registro, especifica el uso de procesador máximo que se debe utilizar para procesar los datos de archivo. Los valores van del 5 al 100 por ciento. El valor predeterminado es el 100 por ciento.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
KUMP_DP_SAMPLE_FACTOR	5	Un entero no negativo	Para un proveedor de datos de archivo de registro, establece el factor de muestreo cuando selecciona **Procesar todos los registros cuando se muestra el archivo** en Agent Builder. Este tiempo asegura que los patrones que abarquen varios registros se escriban antes que se registren las extensiones del patrón.
KUMP_DP_EVENT	5	Un entero no negativo	Para un proveedor de datos de archivo de registro, establece la frecuencia de muestreo para los datos de sucesos, en segundos.
KUMP_DP_FILE_EXIST_WAIT	SÍ	YES, NO	Para un proveedor de datos de archivo de registro, especifica que la hebra de supervisión de archivos continúa ejecutándose si detecta que el archivo supervisado está ausente o vacío. La hebra espera hasta que detecta el archivo, vuelve a realizar la comprobación cada pocos segundos e inicia o reinicia la supervisión cuando el archivo pasa a estar disponible.
KUMP_DP_FILE_SWITCH_ CHECK_INTERVAL	600	Un entero no negativo	La frecuencia en segundos con que el proveedor de datos de archivo de registro busca un archivo de supervisión diferente al conmutar cuando el soporte de nombres de archivo dinámicos está habilitado.
KUMP_DP_FILE_ROW_ PAUSE_INCREMENT	Ninguno	Un entero no negativo	Para un proveedor de datos de archivo de registro, especifica cuántos registros de archivo se leen antes de la pausa en la hebra de supervisión de archivos. La pausa es para que se puedan procesar las actualizaciones anteriores. Utilice esta variable de entorno solo si el archivo supervisado recibe ráfagas de gran volumen de registros nuevos y está preocupado de que algunas actualizaciones de registros puedan perderse.
CDP_COLLECTION_TIMEOUT	60 segundos	Un entero positivo	El número de segundos que el agente espera una respuesta de un recopilador de datos que se ha iniciado en otro proceso. Los recopiladores de datos JMX, JDBC, HTTP y SOAP son algunos ejemplos.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_SSH_TEMP_DIRECTORY	. (punto)	Una cadena de vía de acceso válida en el sistema remoto	Para un proveedor de datos de script SSH habilitado especifica una ubicación en el sistema remoto. Los archivos de script que se proporcionan con el agente se deben cargar en esta ubicación. Una ubicación relativa es relativa para el directorio de inicio del usuario. El valor predeterminado . (punto) indica el directorio de inicio del usuario.
CDP_SSH_DEL_COMMAND	rm -Rf	Una cadena de mandato de supresión válida en el sistema remoto	Para un proveedor de datos de script de SSH habilitado, especifica el mandato para iniciar la supervisión de los archivos de script que se han cargado, proporcionados con el agente con el agente.
CDP_SNMP_SEND_DELAY_FACTOR	0 milisegundos	Un entero positivo	El envío de SNMP inicial se retrasa de 0 al número de milisegundos especificado. Esta variable sólo está habilitada si la agrupación de hebras también está habilitada. El retardo no se aplica a todos los envíos, sólo al primer envío realizado por un grupo de atributos. Esta variable es útil si el dispositivo que se está supervisando a veces puede no responder correctamente si recibe varias solicitudes a la vez.
CDP_ICMP_PING_REFRESH_INTERVAL	60 segundos	Un entero mayor o igual a 1	El ping se ejecuta en los sistemas de un archivo de lista de dispositivos a este intervalo. Si los pings utilizan demasiado tiempo, siempre hay un retraso de por lo menos CDP_PING_MIN_INTERVAL_DELAY segundos antes de que los pings se inicien otra vez. Los datos no se renuevan con más frecuencia que este valor. Los datos se pueden renovar con menos frecuencia en función del número de entradas del archivo de lista de dispositivos y el tiempo que se tarda en recibir respuestas.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_ICMP_PING_MIN_INTERVAL_DELAY	30 segundos	Cualquier entero mayor o igual a 1 y menor que el intervalo de renovación de ping CDP	Después que se ejecuta el ping de los dispositivos en un archivo de lista de dispositivos, el siguiente intervalo de actualización de ping no se inicia hasta que transcurra al menos esta cantidad de segundos.
CDP_ICMP_PING_BURST	10	Un entero mayor o igual a 0	El número de pings que se envían antes que el agente se pause por el tiempo que se especifica la variable CDP_ICMP_PING_BURST_DELAY. Un valor de 0 inhabilita esta función.
CDP_ICMP_PING_BURST_DELAY	10	Un entero mayor o igual a 0	La cantidad de tiempo en milisegundos a esperar después que un número establecido de pings se envíen, tal como lo define la variable CDP_ICMP_PING_BURST. Un valor de 0 inhabilita esta función.
CDP_ICMP_PING_TIMEOUT	2000 milisegundos	Un entero mayor o igual a 1	Número de milisegundos de espera de una respuesta de ping. Este valor se aplica a cada intento de ping que se realice. Los intentos de ping se realizan tres veces para cada host. Si no se recibe ninguna respuesta de cualquiera de los tres intentos, el tiempo total de espera para una respuesta es CDP_ICMP_PING_TIMEOUT multiplicado por 3. De manera predeterminada, este valor es 6000 milisegundos. Si cambia el valor para CDP_ICMP_PING_TIMEOUT, la enumeración predeterminada TIMEOUT para el atributo del tiempo de respuesta actual ya no se aplica. Cambie la enumeración TIMEOUT por el nuevo valor de CDP_ICMP_PING_TIMEOUT multiplicado por 3.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_JDBC_CONNECTIONLESS	falso	true, false	Si se establece en true, las conexiones JDBC se cierran después de cada intento de recopilación de datos. Es decir, todos los grupos de atributos intentan crear su propia conexión cada vez que se recopilan datos. Las conexiones no se vuelven a utilizar si esta variable está habilitada. Si se establece en false, se realiza una conexión a la base de datos y dicha conexión se comparte entre los grupos de atributos.
CDP_SSH_EXCLUDED_ ENVIRONMENT_VARIABLES	Ninguno	Una lista separada por comas de los nombres de variable de entorno	Para un proveedor de datos de script con SSH habilitado, especifica el conjunto de variables de entorno locales que no deben establecerse en el entorno del sistema remoto.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_DP_EVENT_LOG_MAX_BACKLOG_TIME	0 segundos	0, 1 o un entero mayor que 1	Si se establece en 0 y CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS no está establecido en 1 o un entero mayor, no procesa los sucesos que se generan mientras el agente se cierra. 0 es el valor predeterminado. Si está establecido en 1 y CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS no se ha establecido en un entero mayor a 1, procesa todos los sucesos que se genera mientras que el agente se cierra. Si está establecido en un valor mayor a 1 y CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS no se ha establecido en un valor mayor a 1, procesa los sucesos que se generan en el valor en segundos de la hora actual del sistema. Por ejemplo, si el valor se establece en 300, en el inicio, el agente procesa todos los sucesos que se generan en los 300 segundos de la hora actual. Cuando se especifique un valor mayor que 1 para las variables CDP_DP_EVENT_LOG_MAX_BACKLOG_TIME y CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS, se procesa el intervalo de tiempo de sucesos o el número de sucesos. La variable que se elige es la que coincide primero.
CDP_DP_EVENT_LOG_*Reg_Sucesos_Windows*_MAX_BACKLOG_TIME	0 segundos (No procesar sucesos que faltan mientras el agente esté cerrado)	0, 1 o un entero mayor que 1	Si se establece en

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_DP_EVENT_LOG_ MAX_BACKLOG_EVENTS	0 sucesos	0, 1 o un entero mayor que 1	Si se establece en 0 y la variable CDP_DP_EVENT_LOG_MAX_BACKLOG _TIME no se ha establecido en 1 o un entero mayor, no procesa los sucesos que genera mientras el agente se cierra. 0 es el valor predeterminado. Si se establece en 1, y la variable CDP_DP_EVENT_LOG_MAX_BACKLOG _TIME no se ha establecido en un entero mayor a 1, procesa todos los sucesos que se generan mientras el agente se cierra. Si se establece mayor que 1 y CDP_DP_EVENT_LOG_MAX_BACKLOG _TIME no es mayor a 1, procesa como máximo ese número de sucesos que se generan mientras el agente se cierra. Por ejemplo, si el valor se establece en 200, entonces se procesan en el inicio del agente los 200 sucesos que se generaron antes del inicio. Cuando se especifique un valor mayor que 1 para las variables CDP_DP_EVENT_LOG_MAX_BACKLOG _EVENTS y CDP_DP_EVENT_LOG_MAX_BACKLOG _TIME, se procesa ese número de sucesos o ese intervalo de tiempo de sucesos. La variable que se elige es la que coincide primero.
CDP_DP_EVENT_LOG_ *Reg_Sucesos_Windows*_MAX_BA CKLOG_ EVENTS	0 sucesos (No procesar los sucesos que faltan mientras el agente está cerrado)	0 o un entero mayor o igual a 1	Si se establece en
CDP_HTTP_READ_TIMEOUT	10	Un entero positivo	El número de sucesos que se debe esperar por una respuesta a la solicitud de HTTP.
CDP_JAT_THREAD_POOL_SIZE	15	Un entero positivo	El número de hebras que utilizan los proveedores de Java para gestionar solicitudes de recopilación de datos. Los proveedores de datos JMX, JDBC, HTTP y SOAP son los proveedores que se pueden beneficiar de esta agrupación de hebras.

Tabla 259. Variables de entorno. Una tabla que lista las variables de entorno, sus valores predeterminados, los rangos de valores válidos y las descripciones para cada variable *(continuación)*

Variable de entorno	Valor predeterminado	Valores válidos	Descripción
CDP_HTML_OBJECTS_THREAD_POOL_SIZE	10	Un entero positivo	El número de hebras que se utilizan para descargar objetos de páginas que se encuentran en URL supervisadas con el proveedor de datos HTTP.
CDP_HTTP_SOAP_MAX_ROWS	500	Un entero positivo	El número máximo de filas que son devueltas por el proveedor de datos de SOAP de HTTP.
CDP_DP_ALLOW_REMOTE	NO	NO, YES	Si se establece en Sí, el agente permite conexiones de socket remotas. Si se establece en No, el agente permite solo conexiones de socket desde el host local. No es el valor predeterminado.
CDP_DP_INITIAL_COLLECTION_DELAY	varía	Un entero positivo	El número de segundos, después de que el agente se inicia, hasta que la agrupación de hebras empieza su recopilaciones de datos planificadas.

Información sobre proceso de vigilancia

Utilice la página **Información de proceso de vigilancia** para especificar la información de configuración del Agente de proceso de vigilancia.

Acerca de esta tarea

Para abrir la página **Información sobre proceso de vigilancia**, pulse **Información sobre proceso de vigilancia** en la sección **Contenido de agente** de la página **Información de agente**. También puede selecciona el nodo **Información sobre proceso de vigilancia** en la vista Esquema.

Puede especificar la siguiente información de configuración para el proceso de vigilancia del agente:

- **Supervisar a este agente de forma predeterminada**

  Seleccione este recuadro de selección para colocar el agente bajo la gestión de los servicios de gestión de agentes cuando el agente esté instalado. El proceso de vigilancia supervisa si se produce comportamiento malsano o una terminación anómala del agente y lo reinicia.

- **Frecuencia de comprobación (segundos)**

  La frecuencia con la que el proceso de vigilancia comprueba el proceso del agente en busca de comportamientos malsanos o terminaciones anormales. El valor predeterminado es 180 segundos.

- **Número máximo de reinicios**

  Número de veces que el proceso de vigilancia reinicia el agente debido a un comportamiento erróneo o terminación anómala en un período de 24 horas antes de alertar al administrador del problema. El periodo se inicia a medianoche cada día. Así, el primer periodo desde el momento en que se inicia el agente puede ser "corto".

  Se produce un reinicio si el agente cae por alguna razón. El proceso de vigilancia también detiene y reinicia el agente si el agente deja de responder o tiene un comportamiento incorrecto, por ejemplo, si se cruza el umbral de memoria. El valor predeterminado es cuatro reinicios en un periodo de 24 horas; el periodo se calcula entre medianoche y las 11:59 p.m. A medianoche, el recuento de reinicios diarios del agente vuelve a 0 automáticamente.

- **Información sobre umbral de memoria**

Tamaño del proceso de agente (en megabytes) hasta el que puede crecer el agente antes de que su proceso de vigilancia lo considere incorrecto. Existe un valor distinto para Windows, Linux y UNIX. Si el proceso del agente crece por encima del umbral, el proceso de vigilancia detiene el proceso y lo reinicia. No hay ningún valor predeterminado para estas propiedades. Si no se especifica ningún valor, el proceso de vigilancia no supervisa el tamaño del proceso. La medida utiliza el tamaño del conjunto de trabajo en Windows y la memoria de usuario en UNIX y Linux.

Si el proceso de vigilancia detiene al agente y se alcanza el número máximo de reinicios, el proceso de vigilancia envía una alerta de que el agente excedió la cuenta de reinicio y deja de realizar los reinicios automáticos. El proceso de vigilancia seguirá informando si el agente está activo o inactivo suponiendo que se inicie de otra manera, como a través de Tivoli Enterprise Portal.

Debe reiniciar manualmente el agente utilizando el mandato de actuación Iniciar agente de AMS para que el recuento de reinicio no se restablezca.

El recuento se restablece de uno de los siguientes modos (el proceso de vigilancia sigue funcionando y notificando el estado, pero no realiza reinicios automáticos):

- El reloj alcanza la medianoche.
- El usuario utiliza el mandato de actuación AMS Start Agent, que tiene un parámetro de entrada denominado **resetRestartCount**. Si especifica el valor 1 (que significa "true" o "yes"), el recuento de reinicios diarios se restablece en 0.

Para obtener más información, consulte las secciones siguientes en *IBM Tivoli Monitoring: Guía del administrador*:

- Para Tivoli System Monitor Agents

  Configuración de los Servicios de gestión de agentes en Tivoli System Monitor Agents
- Para Tivoli Enterprise Monitoring Agents

  Instalación y configuración de los Servicios de gestión de Tivoli Agent

Información de Cognos

Utilice la página **Información de Cognos** para especificar la información utilizada al generar un modelo de datos Cognos para el agente. Esta información solo se utiliza para el entorno IBM Tivoli Monitoring.

Procedimiento

1. Para abrir la página **Información de Cognos**, pulse **Información de Cognos** en la sección **Contenido de agente** de la página **Información de agente** o el nodo **Información de Cognos** en la Vista de esquema.
2. En el campo **Origen de datos** especifique el nombre del origen de datos que conecta Tivoli Common Reporting con el almacén de datos de IBM Tivoli.

   El valor predeterminado es `TDW`.
3. En el campo **Esquema**, especifique el nombre del esquema de base de datos utilizado para Tivoli Data Warehouse, que se utilizara para calificar completamente los nombres de tablas en los informes de Cognos.

   El valor predeterminado es `ITMUSER`. Este valor se puede cambiar en Framework Manager cuando el modelo de Cognos generado se carga en Framework Manager.

   El recuadro de selección **Añadir este grupo de atributos a una categoría de informes** en la página **Definición de origen de datos** determina donde se coloca el grupo de atributos en el modelo de Cognos. Si no está seleccionado, el grupo de atributos se coloca en la carpeta de atributos ampliados en el modelo de Cognos. Si se selecciona, el grupo de atributos se coloca en la subcarpeta seleccionada (disponibilidad o rendimiento) en la carpeta de Medidas clave. Para obtener más información sobre los campos de origen de datos, consulte Tabla 260 en la página 1229.

Qué hacer a continuación

Puede utilizar el modelo de datos de Cognos para crear informes de Tivoli Common Reporting para el agente, consulte "Generación del modelo de datos de Cognos" en la página 1515.

Enlace con el asistente para generar agente

Cuando haya terminado de crear o de editar el nuevo agente, utilice el asistente para generar agente para preparar la instalación.

Procedimiento

- Cuando haya terminado de crear o de editar el nuevo agente, en la página **Información de agente** de **Agent Editor**, pulse el enlace **Asistente para generar agente**.

  Con el asistente para generar agente puede:

  – Generar los archivos de agente con una instalación de Tivoli Monitoring en el sistema local. Encontrará instrucciones en: "Instalación de un agente localmente" en la página 1427.

  – Crear un paquete para que el agente se pueda instalar en otros sistemas. Encontrará instrucciones en: "Creación del paquete de agente" en la página 1429.

Página Definición de origen de datos

Utilice la página **Definición de origen de datos** para manipular los orígenes de datos.

Acerca de esta tarea

La página **Definición de origen de datos** lista los orígenes de datos que están configurados para el agente. Cuando se selecciona un origen de datos o un atributo en el árbol, la página se actualiza para mostrar las propiedades del objeto seleccionado. Utilice los campos para modificar las propiedades del origen de datos o del atributo seleccionados.

Nota: Para obtener las instrucciones detalladas de creación de orígenes de datos de varios proveedores de datos, consulte "Definición y prueba de orígenes de datos" en la página 1256.

Procedimiento

- Para abrir la página **Definición de origen de datos**, pulse **Orígenes de datos** en la sección **Contenido de agente** de la página **Información de agente** o el nodo **Orígenes de datos** en la vista **Esquema**.
- Puede añadir más orígenes de datos pulsando **Añadir a seleccionados** o pulsando con el botón derecho en el árbol de navegación y seleccionando una de las opciones.
- Puede eliminar orígenes de datos y atributos pulsando con el botón derecho sobre ellos y seleccionando **Eliminar**.
- Se pueden añadir, modificar y eliminar atributos. Para obtener las instrucciones, consulte "Edición del origen de datos y propiedades de atributos" en la página 1228

Copia de orígenes de datos utilizando la página Definición de origen de datos

Utilice la página **Definición de origen de datos** para copiar los orígenes de datos.

Antes de empezar

Vaya a la página **Definición de origen de datos**. Para obtener más información, consulte "Página Definición de origen de datos" en la página 1225

Acerca de esta tarea

Los orígenes de datos que generan grupos de atributos se pueden copiar en el portapapeles y volver a pegar en este agente u otro agente. Los orígenes de datos que no dan como resultado grupos de atributos son los orígenes de datos Disponibilidad y Registro de sucesos de Windows.

Procedimiento

1. Seleccione los grupos de atributos que desea copiar.
2. Corte o copie el grupo de atributos utilizando uno de los métodos siguientes:
   - Pulse **Editar** > **Cortar** > **Editar** > **Copiar** en la barra de menús.
   - Pulse con el botón derecho del ratón uno de los elementos seleccionados y pulse **Cortar** o **Copiar** en el menú.
   - Utilice una de las pulsaciones del sistema operativo o de Eclipse que llaman la acción de cortar o copiar. Por ejemplo, en sistemas Windows, al pulsar **Control-C** se llama la acción de copiar.

   Para eliminar orígenes de datos de su ubicación existente y colocarlos en el portapapeles, utilice **Cortar**. Para colocar los orígenes de datos en su sitio y copiarlos en el portapapeles, utilice **Copiar**.
3. Seleccione el padre de un grupo de atributos (el agente, un subnodo o un grupo de Navigator) o seleccione un grupo de atributos existente.
4. Pegue la selección utilizando una de las opciones siguientes:
   - Seleccione **Editar** > **Pegar** en la barra de menús.
   - Pulse con el botón derecho del ratón en el nodo en el que desea pegar la selección en el árbol, y pulse **Pegar** en el menú.
   - Utilice una de las pulsaciones del sistema operativo o de Eclipse que llaman la acción de pegar. Por ejemplo, en sistemas operativos Windows, al pulsar **Control-V** se llama la acción de pegar.

Resultados

Los grupos de atributos del portapapeles se colocan en el padre seleccionado. De forma alternativa, si un grupo de atributos está seleccionado, los grupos de atributos se colocan en el padre del grupo de atributos seleccionado.

Si hay un conflicto de nombres con otro grupo de atributos durante el pegado, el nombre del grupo de atributos pegado cambia levemente para evitar el conflicto.

Página Información de configuración de tiempo de ejecución

La página **Información de configuración de tiempo de ejecución** muestra las variables de configuración del agente. Pueden definirse los valores de las variables al instalar el agente en un host supervisado.

Estos valores están disponibles para códigos de retorno de mandato y scripts a través del entorno. Para abrir la página **Información de configuración de tiempo de ejecución**, pulse **Configuración de ejecución** en la sección **Contenido del agente** de la página **Información del agente** o el nodo **Configuración de tiempo de ejecución** en la vista Esquema. Agent Builder construye automáticamente el nombre de la variable de entorno a partir del código del producto y de la etiqueta.

Puede añadir y cambiar las propiedades de configuración y proporcionar valores predeterminados utilizando la página **Información de configuración de tiempo de ejecución**.

Página XML de agente del editor

La página **Editor XML del agente** visualiza el XML para la definición del agente.

El XML de la definición del agente incluye la información que se muestra en todas las demás partes de Agent Builder. Si cambia el XML, la información visualizada en Agent Builder refleja el cambio.

Atención: No realice ningún cambio en el XML. Dichos cambios pueden provocar errores que le impidan generar el agente o afectan de forma negativa el funcionamiento del agente.

Cómo guardar las ediciones y los cambios

Los cambios realizados con el editor no se almacenan hasta que los guarde.

Procedimiento

- Guarde de una de las formas siguientes:
  - Seleccione **Archivo** > **Guardar**, seleccionando el icono de guardar (disquete).
  - Pulse **Control+S**

  Al guardar, se produce una validación para asegurar que la información esté completa. Si se produce un problema, se muestra información sobre el error en la vista **Problemas** de Eclipse. Si esta vista no está visible, seleccione **Ventana** > **Mostrar vista** > **Problemas**. Si intenta generar un agente que contenga errores, aparecerá un mensaje de error.

  Nota: Debe corregir todos los errores y guardar los cambios antes de poder generar e instalar el agente.

Confirmación de una versión del agente

Confirme el agente cuando esté seguro de que ha terminado de desarrollar esta versión del agente y está preparado para entregarlo.

Acerca de esta tarea

Los sistemas IBM Tivoli Monitoring requieren que las nuevas versiones de un agente incluyen toda la información incluida en las versiones anteriores de ese agente que se utilizaron en el entorno de supervisión. Incluir toda la información de versiones anteriores es necesario para que los espacios de trabajo, las situaciones y consultas sigan funcionando si el agente nuevo se instala en algunos hosts supervisados, pero el antiguo permanece en los otros.

Tras completar el desarrollo y las pruebas de un agente, debe confirmar el agente como versión final para un número de versión determinado. El Agent Builder garantiza que no se elimina ninguna información tras confirmar el agente. Las compilaciones posteriores del agente tienen un número de versión nuevo.

Existe un límite de 1024 versiones.

Recuerde: Si realiza cambios en un agente que se va a probar y ejecutar en un entorno IBM Cloud Application Performance Management, debe cambiar la versión del agente.

Procedimiento

1. Abra la página **Información de agente** de la ventana **Agent Editor**.
2. En el área **Confirmar versión de agente**, pulse **confirmar este nivel**.
3. Haga una copia de seguridad del agente confirmado o regístrelo en el sistema de control de versiones.

Qué hacer a continuación

Después de confirmar un agente, los cambios adicionales en el agente forma parte de una nueva versión. Debe entrar el nuevo número de versión antes de que los cambios adicionales se puedan guardar. Los cambios en la versión nueva no deben romper la compatibilidad con las versiones anteriores del agente.

Después de confirmar el agente, no puede completar estas acciones en los objetos que ya existían antes de confirmar el agente:

- Suprimir atributos de un grupo de atributos.
- Suprimir grupos de atributos.
- Reordenar los atributos existentes de un grupo de atributos.
- Reorganizar los grupos de atributos existentes (utilizando elementos de Navigator):
- Mover grupos de atributos o grupos de Navigator a subnodos o desde estos.
- Renombrar grupos de atributos.
- Renombrar atributos.
- Cambiar tipos de datos de atributos existentes.

- Cambiar un nombre o tipo de subnodo si contiene un grupo de atributos que existían antes de que se confirmara el agente.
- Cambiar un identificador de empresa o un identificador de agente correspondiente al agente.
- Cambiar el código de producto del agente. Para obtener más información, consulte ("Cambio del código del producto" en la página 1228).

Puede completar las siguientes acciones después de confirmar el agente:

- Añadir atributos nuevos a grupos de atributos existentes.
- Añadir grupos de atributos nuevos.
- Reordenar atributos nuevos.
- Organizar grupos de atributos nuevos utilizando elementos de Navigator.
- Crear tipos de subnodo nuevos.
- Añadir consultas nuevas.
- Añadir situaciones nuevas.
- Añadir espacios de trabajo nuevos.

Establecimiento de un nuevo número de versión del agente

Para guardar los cambios en un agente confirmado, debe especificar el nuevo número de versión.

Procedimiento

1. Abra la página **Información de agente** de la ventana **Agent Editor**.
2. Especifique una versión, fixpack o nivel de parche posterior al nivel actual a continuación de la solicitud de versión.
3. Realice las ediciones en el agente.

   Consejo: Si confirma un agente y olvida cambiar la versión del agente, se le solicitará la nueva versión cuando guarde cualquiera de los cambios.

Cambio del código del producto

Si cambia el código de producto, tendrá un agente incompatible con cualquier versión anterior del agente. Cualquier acción confirmada anterior se perderá y desarrollará un nuevo agente.

Cualquier archivo, situación mandato de actuación o espacios de trabajo que haya exportado desde IBM Tivoli Monitoring e importado al agente se suprimen del agente.

Si intenta cambiar el código de producto de un agente que se ha confirmado, Agent Builder muestra un aviso y le pregunta si desea continuar.

Al pulsar **Sí** en la ventana **Código de producto de agente** recibirá un aviso que indica que el contenido de los archivos de soporte del agente ya no es válido. También recibirá un aviso de que los archivos se eliminarán la próxima vez que se guarde el agente.

Edición del origen de datos y propiedades de atributos

Al añadir orígenes de datos al agente, el Agent Builder crea conjuntos de datos correspondientes. Puede editar los conjuntos de datos y atributos incluidos para proporcionar la información de supervisión necesaria.

Procedimiento

Para editar o eliminar información de un conjunto de datos (grupo de atributos):

1. En el área **Contenido de agente** de la página **Información de agente**, pulse **Orígenes de datos**.

   Se abre la página **Definición de origen de datos**.

2. Seleccione el conjunto de datos (grupo de atributos).

   El área de información del grupo de atributos de la página se actualiza para mostrar las propiedades para el conjunto de datos seleccionado.

   Nota: De forma alternativa, si se encuentra en la última página del asistente de **Agente**, puede efectuar una doble pulsación en el origen de datos para abrir la ventana **Información de grupo de atributos**. Esta ventana tiene la misma información que el área de información del grupo de atributos de la página **Definición de origen de datos**.

   La Tabla 260 en la página 1229 describe la información de campo aplicable a todos los orígenes de datos. Utilice los campos para modificar las propiedades del origen de datos o del atributo seleccionados.

Tabla 260. Campos para editar los orígenes de datos

Nombre del campo	Descripción	Valores aceptables y ejemplos
Nombre de grupo de atributos	El nombre del origen de datos como se visualiza en Tivoli Enterprise Portal o en la consola IBM Cloud Application Performance Management	Valores aceptables: cadena descriptiva menor que o igual a 32 caracteres de longitud. Debe ser exclusivo en el agente. El primer carácter debe ser una letra y los caracteres restantes pueden ser letras, números y caracteres de subrayado. Se muestra un subrayado como espacio. No utilice espacios o caracteres especiales.
Texto de ayuda	Texto de ayuda para el origen de datos	Valores aceptables: cadena de 256 caracteres como máximo.
Produce una sola fila de datos	El origen de datos devuelve una fila de datos. Editable en todos los orígenes de datos muestreados.	Ejemplo: si está supervisando la memoria física del sistema, elija una única fila. Un sistema normalmente gestiona toda su memoria en una única agrupación; por lo que solo se puede devolver una fila de datos.
Puede producir más de una fila de datos	El origen de datos puede devolver cualquier número de filas datos. Editable en todos los orígenes de datos muestreados.	Ejemplo: si está supervisando unidades de disco, elija varias filas porque puede haber más de un disco en un sistema. Para las claves, elija los atributos que distinguen un disco de otro. Para un disco, el atributo clave es un número de disco, una letra de unidad, una etiqueta de volumen o lo que sea adecuado en su entorno.
Produce sucesos	El origen de datos devuelve datos basados en sucesos, una fila de datos por suceso.	Ejemplo: un origen de datos basado en sucesos SNMP envía notificaciones (condiciones de excepción) cuando se cruzan los umbrales de rendimiento. **Nota:** No todos los orígenes de datos pueden producir sucesos.

Tabla 260. Campos para editar los orígenes de datos (continuación)		
Nombre del campo	**Descripción**	**Valores aceptables y ejemplos**
Añadir este grupo de atributos a una categoría de informes	La categoría del modelo generado de Cognos a la que los atributos de este grupo de atributos están asignados.	Marque el recuadro de selección para colocar el grupo de atributos en la subcarpeta seleccionada (Disponibilidad o Rendimiento) en la carpeta Medidas clave. Si el recuadro de selección no está seleccionado, el grupo de atributos se coloca en la carpeta **Medidas ampliadas** en el modelo de datos de Cognos.
Categoría de medida	La categoría a la que los atributos de este grupo de atributos están asignados.	Seleccione **Rendimiento** o **Disponibilidad**.

Nota:

a. Los campos **Producir una única fila de datos** y **Puede producir más de una fila de datos** no afectan a los datos para un origen de datos de sucesos.

b. Para obtener más información sobre tipos de datos muestreados y de sucesos, consulte "Tipos de datos" en la página 1251.

c. Si desea más información sobre los campos de un origen de datos específico, consulte la información del proveedor de datos relevante en "Definición y prueba de orígenes de datos" en la página 1256.

Creación, modificación y supresión de atributos

Puede crear, modificar o suprimir atributos de un conjunto de datos (grupo de atributos).

Para trabajar con atributos, abra la página **Definición de origen de datos**. Para obtener más información, consulte "Página Definición de origen de datos" en la página 1225.

Creación de atributos

Puede añadir atributos nuevos a un conjunto de datos.

Procedimiento

1. Pulse con el botón derecho del ratón sobre el origen de datos y seleccione **Añadir atributo** en el menú.

   Se visualiza la página **Información de atributo**.

   Nota: La página que aparece depende del origen de datos para el atributo.
2. Especifique las opciones para el atributo nuevo en la página **Información de atributo**.

   Consulte "Campos y opciones para definir atributos" en la página 1233 para obtener información sobre los campos y las opciones.
3. Para añadir más atributos, seleccione **Añadir atributos adicionales** y pulse **Siguiente**.
4. Cuando termine de añadir atributos, pulse **Finalizar**.

Copia de atributos

Puede copiar los atributos de la página **Definición de origen de datos**.

Procedimiento

1. En la página **Definición de origen de datos** de Agent Editor, pulse con el botón derecho del ratón sobre el atributo que desee copiar y pulse **Copiar atributo**.
2. En la ventana **Copiar atributo**, escriba el nombre del atributo nuevo en el campo **Nombre** y pulse **Aceptar**.

Edición de atributos

Puede editar y cambiar la información de atributos mediante la página **Definición de origen de datos**.

Procedimiento

1. Seleccione el atributo que desea editar.

   El panel **Información de atributo** de la página se actualiza para mostrar las propiedades del atributo seleccionado.
2. Especifique las opciones para la nueva información de atributo.

   Nota: En la última página del asistente de **Agente** (página **Definición de origen de datos**), puede efectuar una doble pulsación en el atributo para abrir la ventana **Información de atributo**. Esta ventana contiene la misma información que el panel Información de atributo de la página **Definición de origen de datos**.

Creación de atributos derivados

Puede crear un atributo cuyo valor deriva de otros atributos en lugar de derivarse directamente del origen de datos.

Acerca de esta tarea

En el atributo derivado, puede realizar operaciones en los valores de los atributos de origen. Por ejemplo, puede realizar operaciones aritméticas básicas en atributos numéricos o la concatenación de cadenas en atributos de cadenas.

La sintaxis de expresión básica utilizada para expresiones derivadas contiene funciones. Estas funciones proporcionan una manipulación más complicada de datos que incluye la agregación a corto plazo, la conversión de cadena a entero y el acceso a propiedades de configuración y variables de entorno. Además, un editor le ayuda a visualizar la expresión a medida que se crea.

Procedimiento

1. En la página **Definición de origen de datos**, pulse con el botón derecho del ratón en el origen de datos y pulse **Añadir atributo**.
2. En la página **Información de atributo**, escriba un nombre de atributo y el texto de ayuda.
3. Seleccione **Derivado desde otros valores de atributo**.
4. En el campo **Fórmula**, escriba el texto de la fórmula y pulse **Editar** para especificar la fórmula con un editor gráfico.

   Consulte el apartado "Operadores y funciones de fórmula" en la página 1244 para obtener información sobre los operadores y funciones que se pueden utilizar en la fórmula.

   Nota: Al pulsar **Editar**, se abre el editor de fórmulas. Consulte la sección "Edición de atributos derivados" en la página 1233 para ver cómo se editan los atributos derivados.
5. Opcional: Marque o desmarque el recuadro de selección **Cálculos de intervalo específico** para determinar qué dos valores de ejemplo de atributo se utilizan cuando se calcula la función.

   Utilice esta opción cuando la fórmula utiliza la función `rate` o `delta`. Para obtener más información sobre **Cálculos de intervalo específico**, consulte "Cálculos específicos de intervalo" en la página 1232. Para obtener más información sobre las funciones `rate` y `delta`, consulte "Operadores y funciones de fórmula" en la página 1244.
6. En el área **Tipo de atributo**, pulse el tipo de atributo.
7. Pulse **Aceptar**.

La página **Definición de origen de datos** se vuelve a visualizar con el origen de datos incluido en la lista, como antes.

8. Pulse **Finalizar**.

   Importante: Si crea un atributo derivado que hace referencia a otro atributo derivado, asegúrese de que el atributo referenciado se liste antes que el atributo nuevo. Si un atributo hace referencia a otro atributo derivado que aparece más tarde en la lista, el agente no puede visualizar el valor para este atributo. Si crea un atributo así, Agent Builder visualiza un aviso.

Cálculos específicos de intervalo

Puede elegir **Cálculos específicos de intervalo** al definir un atributo derivado basado en las funciones `rate` o `delta`.

Seleccione **Cálculos específicos de intervalo** en el separador **Detalles de atributo derivado** de la página **Información de atributos**. Para obtener más información, consulte "Creación de atributos derivados" en la página 1231.

Cuando se utiliza la selección **Cálculos específicos de intervalo**, es importante comprender el concepto de un delta o la diferencia entre valores de atributo. El delta es la diferencia entre el valor más reciente del atributo y un valor anterior de este. La función `delta` devuelve directamente el delta y la función `rate` lo utiliza para calcular un resultado.

La función `delta` o `rate` siempre debe tener la función `last` como su único argumento. La función `last` especifica qué valores de un atributo se utilizan para determinar el delta. Si **Cálculos específicos de intervalo** no está seleccionado, el valor anterior que se utiliza es siempre el segundo valor más reciente. Si **Cálculos específicos de intervalo** está seleccionado, el valor anterior que se utiliza es el valor cuya edad (en relación con el valor más reciente) es igual al intervalo de recopilación del solicitante.

Por ejemplo, supongamos que `CDP_DP_REFRESH_INTERVAL` se establece en 120 segundos y `attribute A` tiene los siguientes valores muestreados:

Time	**Valor muestreado**
actual	`2800`
hace 2 minutos (120 segundos)	`2600`
hace 4 minutos (240 segundos)	`2499`
hace 6 minutos (360 segundos)	`1500`
hace 8 minutos (480 segundos)	`1200`
hace 10 minutos (600 segundos)	`1000`

Cuando **Cálculos específicos de intervalo** no está seleccionado, la función `delta` siempre devuelve `200`, la diferencia entre los dos valores más recientes, `2800 - 2600`. Se devuelve el mismo valor, independientemente de que el valor se visualice en Tivoli Enterprise Portal o la consola IBM Cloud Application Performance Management, se utilice en una situación o una colección de datos históricos.

Cuando **Cálculos específicos de intervalo** está seleccionado, la función `delta` devuelve un valor que depende del intervalo de recopilación del solicitante.

Si un atributo derivado con la función `delta` se utiliza en una situación con un intervalo de recopilación de 4 minutos, el valor que la función `delta` devuelve es `301`, la diferencia entre el valor más reciente y el valor obtenido 4 minutos antes de eso, `2800 - 2499`.

Si un atributo derivado con la función `rate` se utiliza en una situación con un intervalo de recopilación de 10 minutos (600 segundos), el valor que la función `rate` devuelve es 3, la diferencia entre el valor más reciente y el valor obtenido 10 minutos antes de eso, dividido por el número de segundos en el intervalo `(2800 - 1000) / 600`.

Nota: Tivoli Enterprise Portal no tiene ningún intervalo de recopilación inherente, por lo que los cálculos de delta y rate para las solicitudes deTivoli Enterprise Portal siempre utilizan los valores de atributo más

recientes y segundos más recientes, el mismo resultado si **Cálculos específicos de intervalo** está seleccionado o no.

Para que `delta` o `rate` funcionen correctamente con **Cálculos específicos de intervalo**,

- El agente debe recopilar datos periódicamente en segundo plano y no bajo demanda (`CDP_DP_THREAD_POOL_SIZE` debe ser mayor que 0).
- Cada situación o intervalo de recopilación de datos históricos en el que el atributo se utiliza debe ser un múltiplo del intervalo de renovación en segundo plano (`CDP_DP_REFRESH_INTERVAL`).
- El recuento (el segundo argumento de la última función) debe ser lo suficientemente grande como para acomodar el intervalo de recopilación más grande de una situación o recopilación de datos históricos. Por ejemplo, si el agente debe dar soporte a una recopilación de datos históricos de 10 minutos (600 segundos) y `CDP_DP_REFRESH_INTERVAL` es de 120 segundos, el recuento debe ser como mínimo `6`, `1+(600 / 120)`. Un valor de recuento de 6 garantiza que la función `last` devuelve la muestra más reciente y muestras de hasta 600 segundos.

Nota: Si no se cumplen estas condiciones, es probable que los valores de entrada no sean válidos y que se devuelva un resultado de `0`.

Edición de atributos derivados
Utilice el editor de fórmulas para editar los atributos derivados.

El Editor de fórmulas está disponible en la página **Información de atributo** para un atributo derivado, tal como se describe en “Creación de atributos derivados” en la página 1231. Para obtener más información sobre el Editor de fórmulas, consulte “Editor de fórmulas” en la página 1239

Eliminación de atributos
Puede eliminar uno o varios atributos de un conjunto de datos utilizando la página **Definición de origen de datos**.

Procedimiento

- Para eliminar un atributo o atributos, pulse con el botón derecho del ratón en el atributo o atributos y seleccione **Eliminar** en el menú que se visualiza.

  Nota: No puede eliminar un atributo utilizado por un atributo derivado. Primero debe eliminar la referencia creada por el atributo derivado del atributo que está eliminando.

Campos y opciones para definir atributos
Descripción de la información de campo y las opciones para la página **Información de atributo** que son aplicables a todos los orígenes de datos

Para obtener información sobre la información de campo específica para cada uno de los orígenes de datos, consulte la documentación pertinente para cada origen de datos.

Tabla 261. Campos y opciones para definir atributos		
Nombres de campos/Opciones	**Descripción**	**Valores aceptables**
Nombre de atributo	El nombre del atributo tal cual como se visualiza en Tivoli Enterprise Portal o la consola IBM Cloud Application Performance Management	Cadena con los siguientes caracteres: • A-Z • _ • a-z • 0-9 **Nota:** El nombre debe comenzar por A-Z o a-z. El nombre de atributo tiene un límite de 63 caracteres y el nombre del grupo de atributos tiene un límite de 63 caracteres
Texto de ayuda	Texto de ayuda para el atributo	Serie
Oculto - solo se puede utilizar en atributo derivado	Si está seleccionado, el atributo no se visualiza en Tivoli Enterprise Portal o la consola IBM Cloud Application Performance Management. Consulte la nota en la última fila.	No aplicable
Derivado desde otros valores de atributo	El valor de atributo se va a calcular a partir de valores de otros atributos	No aplicable
Atributo clave	El atributo es una clave en la tabla. Compruebe si este atributo ayuda a definir de forma exclusiva el objeto sobre el que se proporciona información. Si los datos se almacenan y se resumen, los atributos clave se utilizan para resumir datos en las tablas de resumen.	Esta opción no está disponible en atributos de Perfmon.
Panel **Información de atributos**	El contenido de este separador depende del tipo de origen de datos al que pertenece este atributo. Consulte la información de este capítulo sobre el origen de datos que desea supervisar para obtener más información. Para un atributo derivado, en el campo **Fórmula**, especifique una fórmula para calcular el valor del atributo que se basa en otros atributos o constantes. Puede escribir la fórmula en el campo **Fórmula** o pulsar **Editar** para utilizar el editor gráfico de fórmulas. Consulte (“Editor de fórmulas” en la página 1239).	

Tabla 261. Campos y opciones para definir atributos (continuación)		
Nombres de campos/Opciones	**Descripción**	**Valores aceptables**
Tipo de atributo	Describe cómo se visualiza el atributo en Tivoli Enterprise Portal o la consola IBM Cloud Application Performance Management. Hay 3 tipos: • Serie • Numérico • Indicación de fecha y hora "Tipos de atributos" en la página 1235 contiene más información sobre los tipos de atributo.	Tabla 262 en la página 1236 contiene descripciones de los valores de tipo de atributo numérico.
Enumeraciones	Puede ser un valor numérico con escala cero o de cadena	Añada sus enumeraciones a la tabla utilizando el procedimiento en ("Especificación de una enumeración para un atributo" en la página 1238). El nombre de enumeración se visualiza en el Tivoli Enterprise Portal o en la consola IBM Cloud Application Performance Management cuando se recibe el valor correspondiente en el atributo del agente. Este atributo se utiliza para un conjunto de valores específicos con significados identificados (por ejemplo, 1=ARRIBA, 2=ABAJO).
Nota: En los casos donde el atributo se utiliza en cálculos con otros atributos, existen motivos para no mostrar el valor base. Por ejemplo, un número que representa un recuento de bytes se reinicia tan rápido que no tiene muchos usos prácticos.		

Tipos de atributos
Hay tres tipos de atributos

Los tres tipos de atributos son:

- Serie
- Numérico
- Indicación de fecha y hora

Atributos de serie

Al seleccionar **Cadena**, utilice el campo **Tamaño máximo** para especificar la longitud máxima de la cadena en bytes. El tamaño predeterminado es 64 bytes.

Un valor de serie puede contener cualquier carácter UTF-8. El tamaño máximo es la longitud total del almacenamiento intermedio asignado para contener la cadena en bytes. Algunos caracteres UTF-8 no ASCII toman más de 1 byte, de modo que debe tener esto en cuenta cuando seleccione un tamaño

máximo. La agregación de datos en el almacén muestra el valor más reciente recopilado durante el periodo.

Numérico

Al especificar **Numérico**, puede establecer un número de opciones. Consulte Tabla 262 en la página 1236 si desea más información sobre estas opciones.

Indicación de fecha y hora

Un atributo de indicación de fecha y hora es un atributo de cadena con un formato como el siguiente: `CYYMMDDHHMMSSmmm` (donde `C=1` para el siglo XXI). Se deben utilizar los 16 para clientes de scripts o socket. Cuando se visualiza en Tivoli Enterprise Portal o en la consola de IBM Cloud Application Performance Management, se visualiza un tipo de atributo de indicación de fecha y hora en el formato correcto para el entorno local.

Al utilizar la función de búsqueda WMI, el Agent Builder marca automáticamente atributos cuyo tipo CIM es `CIM_DATETIME` como indicaciones de fecha y hora. El proveedor de datos convierte automáticamente atributos WMI a este formato.

Aspectos numéricos de atributos
Descripciones de los aspectos de tamaño, objetivo, escala y rango de los atributos.

Si especifica un atributo numérico, debe especificar el tamaño, la finalidad, la escala y el rango del atributo. Para obtener más información, consulte (Tabla 262 en la página 1236).

Tabla 262. Opciones de atributos numéricos

Aspectos numéricos	Opciones y campos	Descripción
Tamaño	**32 bits** **64 bits**	El valor de los números de 32 bits puede estar en el rango de `-2147483648` a `2147483647` (entre `-2.000.000.000` y `2.000.000.000` aproximadamente). El valor de los números de 64 bits puede estar en el rango de `-9223372036854775808` a `9223372036854775807` (entre $-9x10^{18}$ y $9x10^{18}$ aproximadamente)

Tabla 262. Opciones de atributos numéricos (continuación)

Aspectos numéricos	Opciones y campos	Descripción
Finalidad	**Medidor**	Valores enteros donde los valores sin formato devueltos son mayores o menores que los anteriores. Se admiten valores negativos. Este es el tipo predeterminado para enteros. La agregación de datos en el almacén produce valores de mínimo, máximo y promedio.
	Contador	Valor entero positivo que contiene valores sin formato que generalmente van aumentando con el tiempo. La agregación de datos en el almacén muestra los valores delta total, máximo, mínimo y más reciente. En el ejemplo siguiente de cálculos basados en Delta, los valores de datos detallados de una hora son 9, 15, 12, 20, 22, y el proceso basado en delta tiene las reglas siguientes: • Si el valor actual es mayor o igual que el valor anterior, el resultado es igual al valor anterior menos el valor actual • Si el valor actual es menor que el valor anterior, el resultado es igual al valor actual • Ya que 15 es mayor que 9, el resultado es igual a 6 • Ya que 12 es menor que 15, el resultado es igual a 12 • Ya que 20 es mayor que 12, el resultado es igual a 8 • Ya que 22 es mayor que 20, el resultado es igual a 2 • El valor_TOT es 28, que significa el total de los resultados • El valor_LOW es 2, que es el menor de los resultados • El valor_HI es 12, que es el mayor de los resultados
	Propiedad	Una propiedad del objeto que no cambia con frecuencia. La agregación de datos en el almacén muestra el valor más reciente que se recopila durante el periodo.
	Delta	Valor entero que representa la diferencia entre el valor actual y el valor anterior para este atributo. Debido a que este atributo se representa en forma de medidor en el almacén, la agregación de datos en el almacén produce valores de mínimo, máximo y promedio.
	Cambio de porcentaje	Valor entero que representa el cambio de porcentaje entre el valor actual y el anterior. Este tipo se calcula así: `((nuevo - antiguo)*100)/antiguo`. Ya que este tipo se representa como un indicador en el almacén, la agregación de datos en el almacén produce valores mínimos, máximos y promedio.
	Tipo de cambio	Un valor entero que representa la diferencia entre el valor actual y el valor anterior, el cual se divide por el número de segundos entre las muestras. Convierte un valor (por ejemplo, bytes) en su valor por segundo (bytes por segundo). Ya que este tipo se representa como un indicador en el almacén, la agregación de datos en el almacén produce valores mínimos, máximos y promedio.

Tabla 262. Opciones de atributos numéricos (continuación)		
Aspectos numéricos	**Opciones y campos**	**Descripción**
Escala	**Ajuste decimal**	La escala determina el número de posiciones decimales que tiene el número. Cada posición decimal reduce el rango mencionado anteriormente en un factor de 10. Por ejemplo, un ajuste decimal de 2 muestra dos posiciones decimales, y en un número de 32 bits el rango permitido pasa de ser -21474836.48 a ser 21474836.47. Cuando se especifica un ajuste decimal distinto de cero, el número se manipula internamente como un número de coma flotante. Por lo tanto, es posible que la precisión de números grandes de 64 bits se reduzca.
Rango	**Mínimo** **Máximo**	El rango ofrece el rango esperado del valor. Si no se proporcionan rangos mínimo y máximo, se utilizan los valores máximos mencionados anteriormente. El rango se utiliza para generar una vista inicial más útil en algunas vistas de espacios de trabajo de Tivoli Monitoring.

Especificación de una enumeración para un atributo
Especifique una enumeración de valor mediante la página **Información de atributo**.

Acerca de esta tarea
La especificación de una enumeración para un atributo implica seguir un breve procedimiento. Cuando se encuentra un valor que tiene una enumeración definida, el nombre de la enumeración se visualiza en el Tivoli Enterprise Portal o en la consola de IBM Cloud Application Performance Management, en lugar del valor.

Procedimiento

1. En la página **Información de atributo** área **Tipo de atributo**, pulse **Numérico**.
2. En el área **Enumeraciones**, pulse una enumeración y pulse **Añadir**.
   Se visualiza la página **Definición de enumeración**.
3. Escriba el nombre y el valor de la enumeración en los campos de la ventana.
4. Pulse **Aceptar**.
   A continuación, puede añadir más enumeraciones.

Especificar la gravedad de un atributo utilizado como indicador de estado
En un entorno IBM Cloud Application Performance Management, un panel de instrumentos de resumen debe mostrar un estado. Debe utilizar un atributo para proporcionar el valor del estado. Para este atributo, debe especificar valores que denota la gravedad del estado específico.

Acerca de esta tarea
El atributo que se utiliza para la indicación del estado debe ser numérico. Seleccione este atributo en el asistente **Configuración del panel de instrumentos**; para obtener instrucciones sobre cómo utilizar este asistente, consulte “Preparación del agente para Cloud APM” en la página 1414.

Puede especificar valores para el atributo que corresponden a la gravedad Normal, Aviso y Crítica. Cualquier otro valor denota un estado de gravedad "Desconocido"; también puede definir algunos valores como "No definido" de forma explícita y las interfaces de usuario de estado "Desconocido" visualizadas para estos valores.

Procedimiento

1. Seleccione el atributo que desea editar.

   El panel Información de atributo de la página se actualiza para mostrar las propiedades para el atributo seleccionado.
2. En el panel de información de atributo, pulse la pestaña **Gravedad**.
3. Seleccione la gravedad necesaria (Normal, Aviso, Crítica y No definido) y pulse **Editar**.
4. Seleccione **Rango** o **Número único**, especifique el rango de valores o el valor único numérico y pulse **Aceptar**.
5. Opcional: Si necesita añadir otro valor para la misma gravedad, por ejemplo 2 y 25 denotan Aviso, pulse **Añadir**, seleccione la gravedad, especifique el valor y pulse **Aceptar**.

Filtrado de grupo de atributos

Puede crear un filtro para limitar los datos devueltos desde un grupo de atributos que devuelve datos muestreados.

Antes de empezar

Si el grupo de atributos existe, abra la página **Definición de origen de datos**. Para obtener más información, consulte "Página Definición de origen de datos" en la página 1225.

Si desea crear un grupo de atributos, siga los pasos en "Definición de orígenes de datos iniciales" en la página 1207 y pulse **Avanzado** en la página de información de origen de datos inicial.

Procedimiento

1. Utilice uno de los pasos siguientes para empezar a crear el filtro:
   - Si está creando un grupo de atributos, pulse **Avanzado** en la página de información de origen de datos inicial.
   - Si el grupo de atributos existe, selecciónelo en la página **Definición de origen de datos** y pulse **Avanzado** en la página **Definición de origen de datos**.
2. En la página **Propiedades avanzadas de origen de datos**, entre una fórmula de selección. La fórmula de selección que especifique debe evaluarse en un resultado booleano, true o false.

   En la página **Propiedades avanzadas de origen de datos**, puede pulsar **Editar** para especificar o modificar la fórmula utilizando el Editor de fórmulas. Para obtener más información sobre el Editor de fórmulas, consulte "Editor de fórmulas" en la página 1239
3. Cuando termine de especificar la fórmula de selección de filtros, pulse **Aceptar** hasta que vuelva a la página **Definición de origen de datos**.

   Cuando se crea el filtro, el agente lo utiliza para evaluar cada fila de datos. Cuando el filtro se evalúa como *true* para una fila de datos, los datos se envían a IBM Tivoli Monitoring o IBM Cloud Application Performance Management. Cuando el filtro se evalúa como *false*, la fila de datos no se envía y se descarta.

Qué hacer a continuación

Puede validar que el filtro funciona de la manera prevista utilizando la función de prueba para el grupo de atributos. Para obtener más información sobre la prueba del grupo de atributos, consulte "Prueba de grupo de atributos" en la página 1417

Editor de fórmulas

Utilice el Editor de fórmulas para crear y cambiar fórmulas en Agent Builder.

El Editor de fórmulas, que es una herramienta gráfica, se visualiza cuando realiza una de las siguientes tareas:

1. Crear o editar atributos derivados, consulte “Creación de atributos derivados” en la página 1231 y “Edición de atributos derivados” en la página 1233
2. Crear grupos de atributos filtrados, consulte “Creación de un grupo de atributos filtrado” en la página 1382
3. Filtrar datos de grupos de atributos, consulte “Filtrado de grupo de atributos” en la página 1239

Atención:

- Al crear atributos derivados, la fórmula que crea debe dar como resultado un tipo de datos que coincida con el tipo de atributo. Por ejemplo, si el tipo de atributo derivado es un número, la fórmula que cree debe evaluarse con un resultado numérico.
- Al crear grupos de atributos filtrados o filtrar datos de grupos de atributos, la fórmula que cree debe dar como resultado un valor booleano, "true" o "false".

Nota: En las vistas siguientes, se muestra el editor de fórmulas creando fórmulas para atributos derivados. Las vistas son idénticas cuando utiliza el editor de fórmulas con grupos de atributos filtrados o para filtrar datos de grupos de atributos. Las vistas muestran la cabecera **Editor de fórmulas derivadas** o **Editor de fórmulas filtradas** en función del uso.

Cuando se visualiza el editor de fórmulas, la fórmula actual se carga en el editor. Si una fórmula no existe, puede especificar una escribiendo directamente en el espacio de la fórmula de la ventana **Editor de fórmulas**. De forma alternativa, puede pulsar **Insertar** para especificar una fórmula mediante las opciones de menú del editor. El editor contiene dos vistas de la fórmula en la ventana predeterminada y una opción para una tercera vista:

Vista de componentes (predeterminada)
Los componentes de la fórmula editada se muestran en las áreas de **operando** y el campo **Operador**. El operador y sus dos operandos pueden editarse utilizando los menús de selección.

Vista de fórmulas (predeterminada)
La fórmula completa se encuentra en el campo de la fórmula de la ventana. Puede editar la fórmula escribiendo en este recuadro.

Vista del árbol de jerarquía de fórmulas (opcional)
El árbol de jerarquía de fórmulas se visualiza seleccionando el recuadro de selección **Mostrar jerarquía de fórmulas**. El estado del recuadro de selección se recuerda en las siguientes invocaciones al Editor de fórmulas.

Modificación de la vista de componentes del editor de fórmulas

Modificación de la vista de componentes en el editor de fórmulas.

Acerca de esta tarea

El componente que se muestra en la vista de componentes se puede modificar de las siguientes formas:

Procedimiento

- Mueva el cursor en el texto de la fórmula.
- Seleccione otro nodo en el árbol de jerarquía de fórmulas.
- Seleccione **Subir un nivel** o uno de los botones Editar.

Tipos de componentes

Puede utilizar el Editor de fórmulas para editar el componente actual y los argumentos de función u operandos de ese componente. Algunos componentes pueden aparecer de forma distinta en el Editor de fórmulas cuando se seleccionan.

Componente de atributo del editor de fórmulas

Utilice el componente de atributo en el editor de fórmulas para seleccionar y manipular atributos en la fórmula.

Acerca de esta tarea

Puede seleccionar un atributo en una lista de atributos para el grupo de atributos en la vista de componente del editor de fórmulas.

Procedimiento

1. Para trabajar con un atributo específico, seleccione ese atributo en la lista y pulse **Editar**
   Se visualiza la ventana **Editar el atributo seleccionado**.
2. Puede manipular el atributo seleccionado de las siguientes formas:
   - Puede sustituir el atributo con una cadena o número seleccionando **Cadena** o **Número**. La lista de atributos se sustituye por un campo de entrada y el contenido ya no se compara con la lista de nombres de atributos válidos.
   - Puede sustituir el atributo por una función pulsando **Función**. Se añaden paréntesis después del nombre y la lista contiene nombres de función válidas entre las que se puede elegir.
   - Puede escribir un nombre de atributo en lugar de seleccionarlo. Escribir un nombre es útil si aún no ha definido todos los atributos en este grupo de atributos.
     - Se muestra un aviso si no hay ningún atributo con el nombre especificado.
     - Se muestra un error si se especifican caracteres que no pueden formar parte de un nombre de atributo.
     - El botón **Aceptar** está inhabilitado hasta que se corrija el aviso o el error.
   - Los atributos no se filtran en función del tipo. Si un atributo (o cualquier valor) del tipo incorrecto está seleccionado o especificado, se muestra un mensaje de aviso.

Componentes de literal del editor de fórmulas
Los componentes de cadena y número del Editor de fórmulas se usan para manipular literales en fórmulas.

Acerca de esta tarea

Un literal es cualquier valor que se especifica directamente en la fórmula que no procede de un valor de atributo o de una función. Un valor literal puede ser una cadena o un número.

Procedimiento

- Puede sustituir un número o cadena literal por un atributo pulsando **Atributo**. Un nombre de atributo válido debe seleccionarse o especificarse sin comillas.
- Puede sustituir un número o cadena literal por una función pulsando **Función**. Se añaden paréntesis después del nombre y la lista de selección contiene nombres de función válidos entre los que se puede elegir.
  - Se muestra un aviso si se especifica un número donde debe ir una serie o viceversa.
  - Si **Número** está seleccionado, aparecerá un error si el contenido del campo no es un número. La opción **Aceptar** está inhabilitada hasta que se corrige el error.

Componente de operador del editor de fórmulas
El componente de operador del editor de fórmulas se usa para manipular operadores en las fórmulas.

Acerca de esta tarea

Un componente de operador muestra un operador y sus operandos.

Procedimiento

- En la vista de componente del editor de fórmulas, seleccione el operador de la lista **Operador**, entre los dos operandos. El operador (%) multiplica el primer operando por 100 y luego lo divide por el segundo operando.
- Seleccione el operador (`+ - * / o %`).
  - La sección **Operando izquierdo** de la página está antes del operador.
  - La sección **Operando derecho** está después del operador.
  - Los operandos simples (atributos y literales) se pueden editar sin tener que cambiar el componente seleccionados por el operando tal como se describe en "Componente de atributo del editor de fórmulas" en la página 1240 y "Componentes de literal del editor de fórmulas" en la página 1241.
  - Los operandos complejos, consistentes en otros operadores o funciones, se pueden editar pulsando **Editar**. Esta acción resalta el componente de operando en lugar de todo el operador.

Componente de expresión condicional del Editor de fórmulas

El componente de expresión condicional muestra una condición, un valor que devolver si la condición es verdadera, y un valor que devolver si la condición es falsa.

- La expresión de la sección **Condición** debe evaluarse como verdadera (true) o falsa (false). Los operadores (`==), (!=), (<), (<=), (>), (>=), (&&), (||), (!)`) están disponibles para formar expresiones que devuelvan los valores true o false.
- Los operandos simples (atributos y literales) se pueden editar sin tener que cambiar el componente seleccionados por el operando tal como se describe en "Componente de atributo del editor de fórmulas" en la página 1240 y "Componentes de literal del editor de fórmulas" en la página 1241.
- Los operandos complejos, que se componen de otros operadores o funciones, se pueden editar pulsando el botón Editar. Esta acción resalta el componente de operando en lugar de toda la expresión condicional.
- Consulte la sección "Opciones comunes del Editor de fórmulas" en la página 1243 para ver información sobre cómo utilizar las siguientes opciones: **Insertar**, **Eliminar**, **Subir un nivel** y **Editar**.

Conceptos relacionados

"Editor de fórmulas" en la página 1239
Utilice el Editor de fórmulas para crear y cambiar fórmulas en Agent Builder.

Componente de funciones del editor de fórmulas

El componente de funciones del editor de fórmulas se utiliza para seleccionar y manipular los componentes de función en las fórmulas.

Acerca de esta tarea

El componente de función muestra la función y sus argumentos.

Procedimiento

- Para trabajar con funciones, seleccione el **Nombre de función** en la lista del Editor de fórmulas.
  - La descripción de la función seleccionada se muestra después de la función.
  - Las secciones **Argumento de función** se muestran después del nombre de función. Aparece el número adecuado de argumentos para la función seleccionada. Se muestra una descripción específica de la función seleccionada.
  - Los argumentos simples (atributos y literales) se pueden editar sin tener que cambiar el componente seleccionado por el operando tal como se describe en "Componente de atributo del editor de fórmulas" en la página 1240 y "Componentes de literal del editor de fórmulas" en la página 1241.
  - Los argumentos complejos, consistentes en otros operadores o funciones, se pueden editar pulsando **Editar**. Esta acción resalta el componente de argumento en lugar de toda la función.

- Para las funciones que toman un número variable de argumentos, añada argumentos pulsando **Insertar** o elimine argumentos pulsando **Eliminar** además de las acciones descritas en "Opciones comunes del Editor de fórmulas" en la página 1243.
- Para la función `getenv`, se puede elegir una propiedad de configuración pulsando **Insertar**. Si selecciona la opción Propiedad de configuración, se muestra la ventana **Propiedades de configuración**.

Opciones comunes del Editor de fórmulas
Puede utilizar algunas opciones en todas las vista del editor de fórmulas.

Las opciones comunes del Editor de fórmulas son:

- **Insertar**
- **Eliminar**
- **Subir un nivel**
- **Editar**

Insertar

Insertar inserta un operador o una función antes del componente. El componente se rebaja a uno de los operandos del operador o a uno de los argumentos de la función. Por ejemplo, si pulsa **Insertar** antes de la función `sqrt(attr2)`, se le preguntará qué desea insertar y se visualizarán las opciones siguientes:

- **Un operador con sqrt(attr2) como uno de los operandos del operador**
- **Una función con sqrt(attr2) como primer argumento de la función**
- **Una expresión condicional con sqrt(attr2) como los valores true o false**

Si pulsa **Insertar** antes de la función `getenv`, se le preguntará si desea insertar y se visualizarán las siguientes opciones:

- **Propiedad de configuración**: utilice esta opción para recuperar el valor de una propiedad de configuración que ha configurado para el agente, o cualquiera de las variables de entorno (por ejemplo, `JAVA_HOME`) en el host que ejecuta el agente.
- **Un operador con attr2 como uno de los operandos del operador**
- **Una función con attr2 como el primer argumento de la función**
- **Una expresión condicional attr2 como los valores true o false**

Eliminar

Eliminar solo está disponible para operadores y funciones y es el inverso de **Insertar**. Cuando pulsa **Eliminar**, se le solicita qué se debe utilizar para sustituir el operador o la función eliminados. Por ejemplo, **Eliminar** antes de la función `sqrt(attr2)` muestra las siguientes opciones:

- **El argumento actual 1, attr2**
- **Una serie, número o referencia de atributo nuevo**

Seleccione **Una serie, número o referencia de atributo nuevo** para descartar todo el árbol después del punto que se está eliminando y sustitúyalo con un valor nuevo de atributo o literal.

Pulse **El argumento actual** para ascender el operando o argumento seleccionado para sustituir el operador o la función que se ha eliminado. Puede pulsar las opciones posteriores si hay más argumentos u operandos. Cualquier otro operando o argumento se descarta.

Subir un nivel

Pulse **Subir un nivel** para subir en el árbol.

Editar

Pulse **Editar**, antes de un operando o argumento complejo, para que sea el componente que se va a editar.

Pulse **Subir un nivel** después de pulsar **Editar** para restaurar el componente actual al estado en que estaba antes de pulsar **Editar**.

Editor de fórmulas - Errores de fórmulas
Corrección de errores de fórmulas en el **Editor de fórmulas**

La vista de componente es distinta cuando no hay ninguna fórmula o cuando no se puede analizar la fórmula completa. No muestra un árbol de fórmula. En lugar de esto, muestra un mensaje de error.

Puede corregir una fórmula con errores de análisis escribiendo directamente en el campo de la fórmula o sustituyéndola por una nueva fórmula pulsando **Insertar**. En este caso, **Insertar** presenta las siguientes opciones:

- **Un atributo**
- **Una cadena**
- **Un número**
- **Un operador**
- **Una expresión condicional**
- **Una función**

Conceptos relacionados
“Editor de fórmulas” en la página 1239
Utilice el Editor de fórmulas para crear y cambiar fórmulas en Agent Builder.

Operadores y funciones de fórmula

Una referencia (que incluye ejemplos) de operadores y funciones de fórmula que se utilizan en el editor de fórmulas.

Un valor de atributo derivado es el resultado de evaluar una expresión basada en constantes y otros valores de atributo del mismo origen de datos. La gramática de la expresión es la expresión matemática normal: operando operador operando con los paréntesis para agruparlos. Los atributos numéricos se pueden combinar con otros atributos numéricos o constantes utilizando los operadores matemáticos normales: `+ - * / y %`, que multiplica el **operando izquierdo** por 100 y lo divide por el **operando derecho**. Los atributos de cadena se pueden combinar con otros atributos de cadena o constantes con +. También puede utilizar las siguientes funciones descritas. Las funciones se especifican con el formato: `nombre_función(argumento_1, argumento_2, argumento_3)`.

Un atributo se representa por su nombre (el mismo nombre que se ve en el árbol **Información de origen de datos**). Las contantes enteras se especifican como números. Las constantes de series se especifican entre comillas.

Puede realizar las siguientes funciones en una fórmula:

abs
Devuelve el valor absoluto de un número

atof
Convierte una serie en un valor de coma flotante

atoi
Convierte una serie en un valor entero. Funciona del mismo modo que la función **C atoi** normal; se detiene cuando encuentra el primer carácter no decimal.

average
Devuelve un solo valor que es el promedio de un conjunto de valores. El conjunto de valores procede de los argumentos de la función. Se pueden proporcionar varios valores individuales (por ejemplo, nombres de atributos y constantes), cada uno en un argumento separado. De forma alternativa, la

última función puede ser el único argumento para esta función (para calcular el promedio de los valores más recientes de un atributo).

Ejemplos de esta función en uso son:

```
average (Attr_A, AttrB, Attr_C)
```

```
average (last (Attr_A, 10))
```

ceiling
Devuelve el entero más pequeño que no es menor que el argumento.

Por ejemplo, donde `attribute_a = 12.4`, `ceiling(attribute_a)` devuelve el valor 13. Y donde `attribute_a = -12.4`, `ceiling(attribute_a)` devuelve el valor `-12`.

delta
La diferencia entre el valor más reciente de un atributo y un valor recopilado anteriormente de ese atributo. El único argumento para delta debe ser la función `last`, que obtiene los valores anteriores y actuales de un atributo. Un uso normal podría parecerse a:

```
delta (last(OtherAttribute, 2))
```

Para obtener más información sobre qué valores de atributo de la función last se utilizan para calcular el delta, consulte “Cálculos específicos de intervalo” en la página 1232. Esta función solo es aplicable para atributos derivados, no para filtros de grupos de atributo.

floor
Devuelve el entero más grande que no es mayor que el argumento.

Por ejemplo, donde `attribute_a = 12.4`, `floor(attribute_a)` devuelve el valor 12. Y donde `attribute_a = -12.4`, `floor(attribute_a)` devuelve el valor `-13`.

getenv
Devuelve el valor del entorno proporcionado o la "variable de configuración".

ipAddressToName
Convierte una dirección IP en un nombre de host. Esta función requiere un argumento, una cadena de dirección IP en notación decimal con puntos. Si la dirección no se puede resolver, se devuelve la dirección IP.

itoa
Convierte un entero en una serie. Esta función resulta muy útil si desea concatenar un valor numérico en una serie. La función + de cadena derivada solo toma dos argumentos de cadena.

last
Devuelve una lista de valores para que los utilicen las funciones `min`, `max`, `average`, `stddev`, `rate` y `delta`. Toma dos argumentos: el atributo que se debe recopilar y el número de valores que se deben utilizar en el cálculo. Si el atributo necesario es un valor entero en un atributo de cadena, el primer argumento puede contener la función `atoi`, como `atoi(numericalStringAttribute)`. El segundo argumento debe ser un número. Puede codificarse como una constante o puede ser el resultado de una expresión `atoi(getenv("ENV_VAR"))`. No puede hacer referencia a un valor de atributo.

Ejemplos de esta función en uso son:

```
average (last (Attr_A, 10))
```

```
last (Attribute_A, ${K01_NUM_COLLECTIONS}))
```

Restricción: Puede utilizar la función `last` solo una vez en una fórmula específica.

matches
Devuelve un valor booleano, true o false, que indica si una expresión regular coincide con un valor. Toma dos argumentos, el origen de serie y una expresión regular, cuyo resultado se compara con la serie. Esta función es útil para filtrar grupos de atributos.

max
Devuelve un solo valor que es el máximo de un conjunto de valores. El conjunto de valores procede de los argumentos de la función. Se pueden proporcionar varios valores individuales (por ejemplo, nombres de atributos y constantes), cada uno en un argumento separado. De forma alternativa, la última función puede ser el único argumento para esta función (para calcular el máximo de los valores más recientes de un atributo).

min.
Devuelve un solo valor que es el mínimo de un conjunto de valores. El conjunto de valores procede de los argumentos de la función. Se pueden proporcionar varios valores individuales (por ejemplo, nombres de atributos y constantes), cada uno en un argumento separado. De forma alternativa, la última función puede ser el único argumento para esta función (para calcular el mínimo de los valores más recientes de un atributo).

nameToIpAddress
Convierte un nombre de host a una dirección IP. Esta función requiere un argumento, una serie de nombre de host. Si la dirección no se puede resolver, se devuelve el nombre de host.

NetWareTimeToTivoliTimestamp
Convierte un valor de tiempo hexadecimal de Novell NetWare en una indicación de fecha y hora de Tivoli Monitoring. Esta función requiere un argumento, un valor de tiempo hexadecimal de NetWare hexadecimal especial. El tipo de atributo es indicación de fecha y hora.

rate
La frecuencia de cambio (por segundo) entre el valor más reciente de un atributo y un valor recopilado anteriormente de ese atributo. El único argumento para rate debe ser la función `last`, que contiene los valores anteriores y actuales de un atributo. Un uso normal podría parecerse a:

```
rate (last(OtherAttribute, 2))
```

Para obtener más información sobre qué valores de atributo de la función last se utilizan para calcular la frecuencia, consulte“Cálculos específicos de intervalo” en la página 1232. Esta función solo es aplicable para atributos derivados, no para filtros de grupos de atributo.

replaceFirst
Sustituye la primera aparición de una subserie que coincide con una expresión regular por una cadena de sustitución. Esta función toma tres argumentos. Primero: la serie de entrada. Segundo: la expresión regular que se utiliza para comparar una subcadena en la cadena de entrada. Tercero: la cadena de sustitución. Consulte (“Expresiones regulares de ICU” en la página 1530) para obtener detalles sobre las expresiones regulares y valores de sustitución que se permiten en la cadena de sustitución.

replaceAll
Sustituye todas las apariciones de subcadenas que coincide con una expresión regular por una cadena de sustitución. Esta función toma tres argumentos. Primero: la serie de entrada. Segundo: la expresión regular que se utiliza para comparar una subcadena en la cadena de entrada. Tercero: la cadena de sustitución. Consulte (“Expresiones regulares de ICU” en la página 1530) para obtener detalles sobre las expresiones regulares y valores de sustitución que se permiten en la cadena de sustitución.

round
Redondea matemáticamente el número al número entero más cercano.

sqrt
Devuelve la raíz cuadrada de un número

stddev
Devuelve un solo valor que es la desviación estándar de un conjunto de valores. El conjunto de valores procede de los argumentos de la función. Se pueden proporcionar varios valores individuales (por ejemplo, nombres de atributos y constantes), cada uno en un argumento separado. De forma alternativa, la última función puede ser el único argumento para esta función (para calcular la desviación estándar de los valores más recientes de un atributo).

StringToTivoliTimestamp

Convierte una cadena de fecha y hora en una indicación de fecha y hora de Tivoli Monitoring. Esta función requiere dos argumentos. El primer argumento es una representación de cadenas de formato libre de la indicación de fecha y hora. El segundo argumento es una cadena de formato que identifique cómo analizar la representación de cadenas de formato libre de una indicación de fecha y hora. La Tabla 263 en la página 1247 describe los parámetros de formato válidos. El tipo de atributo es indicación de fecha y hora.

Tabla 263. Parámetros de formato válidos para StringToTivoliTimestamp

Símbolo	Significado	Formato	Ejemplo
y	Año	yy yyyy	*96* *1996*
M	Mes **Nota:** Sólo se da soporte a las cadenas de mes en inglés.	M o MM MMM MMMM	*09* *Sept* *Septiembre*
d	día	d dd	*2* *02*
E	Día de la semana **Nota:** Sólo se da soporte a las cadenas de día de la semana en inglés.	EE EEE EEEE	*Sa* *Sáb* *Sábado*
h	Hora en AM o PM (1-12)	hh	*07*
H	Hora del día (0-23)	HH	*00*
m	Minuto de la hora	mm	*04*
s	Segundo del minuto	ss	*05*
S	Milisegundo	S SS SSS	*2* *24* *245*
a	marcador AM o PM	a o aa	*am*
Cualquier otro carácter ASCII	sáltese este carácter	- (guión) (espacio) / (barra inclinada) : (dos puntos) * (asterisco) , (coma)	

Tabla 264 en la página 1248 proporciona ejemplos de representaciones de cadena de indicaciones de fecha y hora y las cadenas de formato que se utilizan para analizarlas.

Tabla 264. Ejemplos de StringToTivoliTimestamp. Una tabla que lista y explica unos pocos ejemplos de representaciones de cadena de indicaciones de fecha y hora.

Representación de cadena de la indicación de fecha y hora	**Cadena de formato**
96.07.10 at 15:08:56	`yy.MM.dd ** HH:mm:ss`
Wed, August 10, 2010 12:08 pm	`EEE, MMMM dd, yyyy hh:mm a`
Thu 21/01/2010 14:10:33.17	`EEE dd/MM/yyyy HH:mm:ss.SS`

sum
Devuelve un solo valor que es la suma de un conjunto de valores. El conjunto de valores procede de los argumentos de la función. Se pueden proporcionar varios valores individuales (por ejemplo, nombres de atributos y constantes), cada uno en un argumento separado. De forma alternativa, la última función puede ser el único argumento para esta función (para calcular la suma de los valores más recientes de un atributo).

TivoliLogTimeToTivoliTimestamp
Convierte una indicación de tiempo y hora de archivo de registro de Tivoli en una indicación de fecha y hora de Tivoli Monitoring. Esta función requiere un argumento, la cadena de indicación de fecha y hora de un archivo de registro de Tivoli. El tipo de atributo es indicación de fecha y hora.

tokenize
Señal de una cadena señalizada. Este función requiere tres argumentos. El primer argumento es una cadena que se divide en señales. El segundo argumento ofrece uno o más caracteres en la cadena que separan una señal de otra. Cualquier aparición de los caracteres de este argumento se utiliza para identificar y separar señales en el primer argumento. El tercer argumento es el índice de la señal que devolver como resultado de esta función. La primera señal es el índice 0, la segunda señal es el índice 1, etc. Este argumento también puede ser una cadena LAST para devolver la última señal.

UTCtoGMT
Convierte la hora universal coordinada en una indicación de tiempo y hora de Tivoli Monitoring GMT. Esta función requiere un argumento, el valor time_t entero. El tipo de atributo es indicación de fecha y hora.

UTCtoLocalTime
Convierte la hora universal coordinada en una indicación de fecha y hora de Tivoli Monitoring local. Esta función requiere un argumento, el valor time_t entero. El tipo de atributo es indicación de fecha y hora.

Las funciones siguientes no toman argumentos y devuelven un número.

count
Mantiene un contador que comienza en 1 la primera vez que se le llama y se incrementa en 1 con cada llamada siguiente. Si lo utiliza en una expresión que también utiliza `last`, coincide con el número de elementos almacenados por `last()`, pero solo hasta que `last()` alcance su máximo. En este momento, `last()` empieza a suprimir el valor más antiguo por cada nuevo valor, manteniendo el mismo número de valores totales, mientras que `count()` siempre aumenta.

cumulativeSum
Devuelve la suma de valores de argumento de sucesos duplicados representados por un suceso de resumen de control de flujo. O bien devuelve el argumento si es un único suceso de un origen de datos. Solo toma un argumento numérico. Esta función solo se aplica a grupos de atributos de sucesos con el `filtrado de sucesos` y el resumen activados.

eventThreshold
Devuelve el valor de umbral configurado para el grupo de atributos que ha generado el suceso. Un número, con tres enumeraciones:

- `SEND_ALL (-3)`

- SEND_FIRST (-2)
- SEND_NONE (-1)

El número entre paréntesis es el valor sin formato. Sin embargo, el Agent Builder define las enumeraciones, así pues, de forma predeterminada, la versión de texto es visible en el Tivoli Enterprise Portal o en la consola de IBM Cloud Application Performance Management. Si especifica un umbral numérico real y no una de las tres opciones predefinidas, esta función devuelve dicho número. El formato del valor es un entero > 0. Esta función solo se aplica a grupos de atributos de sucesos con el `filtrado de sucesos` y el resumen activados.

isSummaryEvent
Devuelve 0 si se trata de un solo suceso procedente de un origen de datos o 1 si el suceso es un suceso de resumen de control de flujo. Los valores visualizados sin Suceso y Suceso de resumen si utiliza el atributo predeterminado para la función. Si crea el atributo manualmente, los valores visualizados son 0 y 1, a no ser que defina los nombres como enumeraciones. Esta función solo se aplica a grupos de atributos de sucesos con el `filtrado de sucesos` y el resumen activados.

occurrenceCount
El número de sucesos coincidentes representados por un suceso de resumen de control de flujo, o 1 si es un único suceso de un origen de datos. (Un suceso de resumen de control de flujo incluye el primer suceso). Esta función solo se aplica a grupos de atributos de sucesos con el `filtrado de sucesos` y el resumen activados.

summaryInterval
Devuelve el intervalo de resumen configurado para el grupo de atributos que ha generado el suceso, en segundos. Esta función solo se aplica a grupos de atributos de sucesos con el `filtrado de sucesos` y el resumen activados.

Ejemplos

Ejemplos de la utilización de operadores y funciones de fórmula para crear atributos derivados y filtrados

Ejemplo 1 - Atributos derivados

Si tiene un origen de datos que define el tipo de atributo siguiente:

Nombre	Serie
xBytes	Numérico
yBytes	Numérico
Virtual_Size	Numérico

Pueden definirse:

- Un atributo `totalBytes` que sea la suma de `xBytes` y `yBytes`. Especifique la fórmula `xBytes + yBytes`.
- Un atributo `yPercent` que sea un porcentaje del total de bytes, que es `yBytes`, se puede definir como `yBytes % (xBytes + yBytes)` o `yBytes % totalBytes`.

Ejemplo 2 - Atributos derivados

Esta fórmula devuelve el máximo de valores recopilados recientemente para el atributo `Virtual_Size`. El número de muestras que se recopilan es el valor de la variable de configuración, *K4P_COLLECTIONS_PER_HISTORY_INTERVAL* (a la que se accede mediante `getenv`), convertido en un número (mediante `atoi`):

```
max(last(Virtual_Size,atoi(getenv("K4P_COLLECTIONS_PER_HISTORY_INTERVAL"))))
```

Ejemplo 3 - Atributos derivados

Esta fórmula devuelve la raíz cuadrada de la suma de los cuadrados de los valores de atributo `xBytes` y `yBytes`:

```
sqrt(xBytes * xBytes + yBtyes * yBytes)
```

Ejemplo 4 - Atributos derivados

Esta fórmula devuelve el promedio del atributo `xBytes` de las 20 muestras más recientes del grupo de atributos. Si se han recopilado menos de 20 muestras desde que se ha iniciado el agente, devuelve el promedio del atributo `xBytes` de todas las muestras:

```
average(last(xBytes,20))
```

Ejemplo 5 - Atributos filtrados

Tiene un origen de datos que devuelve:

```
Nombre  Tipo  Tamaño  Utilizado  Libre
Memoria MEM      8     4     4
Disco1  DISK   300   200   100
Disco2  DISK   500   100   400
```

Sólo le interesa el uso de disco. La solución consiste en crear un filtro para limitar los datos que se devuelven. Para limitar los datos devueltos, se crea un filtro simple que devuelve un valor booleano, true o false, de la siguiente manera

Filtro de disco:

```
Type=="DISK"
```

Ahora cuando el filtro `Type=="DISK"` es true, el grupo de atributos devuelve los datos de uso de disco, por ejemplo:

```
Nombre  Tipo  Tamaño  Utilizado  Libre
Disco1  DISK   300   200   100
Disco2  DISK   500   100   400
```

Ejemplo 6 - Atributos filtrados

Tiene un origen de datos que devuelve:

```
Nombre Tamaño  Utilizado  Libre
Memoria   8     4     4
Disco1  300   200   100
Disco2  500   100   400
```

son similares al ejemplo anterior, sin embargo, no hay un atributo `Type` presente esta vez. Aquí puede utilizar la función matches para buscar cualquier fila de datos con un valor de atributo de nombre que coincida con `"Disk"`, seguido de un número.

Filtro de disco:

```
matches(Name, "Disk[0-9]*")
```

Ahora cuando el filtro coincide con la cadena `"Disk"` seguida por un número en el atributo `Name`, solo se devuelven las filas de datos de uso de disco:

```
Nombre Tamaño  Utilizado  Libre
Disco1  300   200   100
Disco2  500   100   400
```

Especificación de sistemas operativos

Cuando se definen orígenes de datos que no están disponibles en todos los sistemas operativos soportados por el agente, hay que especificar los sistemas operativos en los que ejecuta el origen de datos.

Acerca de esta tarea

De forma predeterminada, el origen de datos proporciona datos en todos los sistemas operativos definidos a nivel de agente, tal como se describe en "Sistemas operativos predeterminados" en la página 1210. Puede cambiar los sistemas operativos para cada origen de datos.

Procedimiento

1. Para abrir la sección Sistemas operativos, pulse **Sistemas operativos** en la página **Información de origen de datos** cuando añade un origen de datos.
2. Seleccione los sistemas operativos en los que tiene que operar el origen de datos.

   Seleccione sistemas operativos individuales, todos los sistemas operativos, todos los sistemas operativos de un tipo específico, o los sistemas operativos predeterminados del agente.

Configuración y ajuste de la recopilación de datos

Cuando se crea un agente de Agent Builder, puede configurar y ajustar la recopilación de datos para obtener los mejores resultados.

La forma de configurar y ajustar el agente puede variar para diferentes agentes de Agent Builder e incluso entre grupos de atributos en un único agente. Los agentes de Agent Builder pueden incluir dos tipos de datos y soportan dos métodos básicos de recopilación de datos para los tipos de datos más comunes.

Tipos de datos

Un agente recopila dos tipos de datos:

1. La mayoría de los grupos de atributo de Tivoli Monitoring representan instantáneas de los datos. Alguien pide los datos y se devuelve. Los agentes utilizan este tipo de datos para representar información de configuración, rendimiento, estado y más donde una colección de un momento de un conjunto de datos tiene sentido. Estos datos se denominan *datos de ejemplo*.
2. Algunos datos de Tivoli Monitoring representan sucesos. En este caso, un suceso ocurre y el agente debe reenviar los datos a Tivoli Monitoring. Algunos ejemplos de suceso son condiciones de excepción SNMP, entradas de registro de suceso de Windows y nuevos registros que se escriben en un archivo de registro. Para simplificar, estos tipos de datos se agrupan y se los denomina *datos de suceso*.

Datos de ejemplo

Cuando se necesitan datos de ejemplo, se envía una solicitud al agente para un grupo de atributos específico. La solicitud se puede iniciar pulsando un espacio de trabajo en Tivoli Enterprise Portal. Una situación que está en ejecución, una recopilación de datos para el almacén o una solicitud de SOAP también pueden iniciar una solicitud. Cuando el agente recibe la solicitud, devuelve los datos actuales para ese grupo de atributos. Tivoli Enterprise Portal solicita establecer como destino un grupo de atributos específico en un determinado Nombre de sistema gestionado (MSN). Las solicitudes históricas y de situaciones son más interesantes, especialmente en un agente que incluye subnodos. Cuando una situación necesita datos para un grupo de atributos en un subnodo, el agente recibe una solicitud con una lista de los subnodos de destino. El agente debe responder con todos los datos del grupo de atributos solicitado para todos los subnodos antes que Tivoli Monitoring pueda trabajar en la siguiente solicitud.

La manera más directa de que un agente cumpla con una solicitud es recopilar los datos cada vez que recibe una solicitud de Tivoli Monitoring. Los agentes de Agent Builder no recopilan datos cada vez. Los datos no se recopilan cada vez porque a menudo la recopilación de datos requiere tiempo o recursos. Y en muchos casos se solicitan los mismos datos muchas veces en poco tiempo. Por ejemplo, un usuario puede definir varias situaciones que se ejecutan en el mismo intervalo en un grupo de atributos y las situaciones pueden señalar condiciones diferentes. Cada una de estas situaciones genera una solicitud

para el agente, pero es posible que prefiera que cada una de ellas viera los mismos datos. Es probable que, ya que cada situación ve los mismos datos, se obtengan resultados más consistentes y que el agente de supervisión minimice la demanda de los recursos de sistema.

El desarrollador de agentes puede configurar agentes para optimizar la recopilación de datos si selecciona ejecutar la recopilación en una de las dos modalidades siguientes:

1. **Recopilación bajo demanda**: el agente recopila datos cuando recibe una solicitud y devuelve esos datos.
2. **Recopilación planificada**: el agente ejecuta la recopilación de datos en segundo plano en intervalos planificados y devuelve los datos recopilados más recientemente cuando recibe una solicitud.

El agente utiliza una memoria caché de corto plazo en ambas modalidades. Si se recibe otra solicitud de datos cuando la memoria caché es válida, el agente devuelve los datos de la memoria caché sin recopilar datos nuevos para cada solicitud. Utilizar datos de la memoria caché resuelve el problema que causan las solicitudes de situaciones de simultáneas múltiples (y de otro tipo). Las variables de entorno definen la cantidad de tiempo que los datos son válidos, el intervalo de recopilación planificada, el número de hebras que se utilizan para la recopilación y si el agente se ejecuta bajo demanda o en modalidad planificada. Mediante las variable de entorno, puede ajustar cada agente para obtener su mejor funcionamiento en su entorno.

Vea los siguientes ejemplos que ilustran cómo funcionan los agentes en ambas modalidades:

- Agente 1 (recopilación *bajo demanda*): Un agente simple que recopila una pequeña cantidad de datos que es normalmente accesible solo a situaciones o en una base poco frecuente en el Tivoli Enterprise Portal. La recopilación de datos es bastante rápida, pero puede consumir recursos informáticos y de redes. Este agente normalmente está definido para ejecutarse on demand. Si no se ejecutan situaciones o nadie pulsa Tivoli Enterprise Portal, el agente no realiza ninguna acción. Cuando se necesitan datos, estos se recopilan y se devuelven. Los datos son colocados en la memoria caché de corto plazo de manera que futuras solicitudes realizadas al mismo tiempo devuelvan los mismos datos. Este tipo de recopilación probablemente es el modo más eficiente para ejecutar el agente puesto que recopila datos sólo cuando alguien realmente los necesita.
- Agente 2 (recopilación *planificada*): un agente complejo que incluye subnodos y recopila datos de varias copias del recurso supervisado. Un agente puede gestionar muchas copias del recurso. Es normal ejecutar situaciones en los datos con bastante frecuencia para supervisar el estado y el rendimiento del recurso supervisado. Este agente se define para ejecutar una recopilación *planificada*. Una razón para ejecutar una colección *planificada* es la forma en que las situaciones se evalúan mediante los agentes de Tivoli Monitoring. Como las situaciones se ejecutan en los grupos de atributos en los subnodos, el agente recibe una solicitud de datos de todos los subnodos simultáneamente. El agente no puede responder a otras solicitudes hasta que se devuelvan todos los datos para una situación. Si el agente recopiló todos los datos cuando llegó la solicitud, el agente se bloqueará cuando pulse uno de los espacios de trabajo en Tivoli Enterprise Portal. Para evitar bloquear el agente, Agent Builder define automáticamente que todos los agentes de subnodo para que se ejecuten como recopilación planificada. El desarrollador de agente ajusta el número de hebras y el intervalo de actualización para recopilar los datos en un intervalo razonable para el tipo de datos. Por ejemplo, el intervalo de renovación puede ser una vez por minuto, o una vez cada 5 minutos.

Variables de entorno

Un agente determina la modalidad que utilizará y cómo se ejecuta la recopilación de datos planificada en función de los valores de un conjunto de variables de entorno. Estas variables de entorno pueden configurarse en la definición del agente en el panel **Variables de entorno**. Cada variable de entorno se lista en el menú junto con los valores predeterminados. Las variables de entorno pueden configurarse o modificarse para un agente instalado mediante la edición del archivo de entorno del agente (`env`) en Windows o el archivo de inicialización en (`ini`) UNIX. Las variables de entorno que controlan las recopilaciones de datos para los grupos de atributos de muestra son:

- `CDP_DP_CACHE_TTL=<periodo de validación para los datos de la memoria caché - valor predeterminado de 55 segundos>`

- CDP_DP_THREAD_POOL_SIZE=<número de hebras que se utilizarán en la recopilación simultánea - el valor predeterminado es 15 para agentes del subnodo>
- CDP_DP_REFRESH_INTERVAL=<número de segundos entre recopilaciones - el valor predeterminado es 60 segundos para agentes del subnodo>
- CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT=<cantidad de tiempo de espera para que caduquen los datos nuevos tras el periodo de validación, el valor predeterminado es 5 segundos>

Las variables más importantes son CDP_DP_CACHE_TTL, CDP_DP_REFRESH_INTERVAL y CDP_DP_THREAD_POOL_SIZE.

Si CDP_DP_THREAD_POOL_SIZE tiene un valor mayor que o igual a 1 o el agente incluye subnodos, el agente opera en modalidad de recopilación *planificada*. Si CDP_DP_THREAD_POOL_SIZE no se ha establecido o es 0, el agente se ejecuta en la modalidad de recopilación *bajo demanda*.

Si el agente se ejecuta en modalidad *planificada*, el agente recopila automáticamente todos los grupos de atributos cada CDP_DP_REFRESH_INTERVAL segundos. Utiliza un conjunto de hebras de fondos para recopilar. El número de hebras se establece mediante CDP_DP_THREAD_POOL_SIZE. El valor correcto para CDP_DP_THREAD_POOL_SIZE varía en función de lo que el agente está haciendo. Por ejemplo:

- Si el agente recopila datos de sistemas remotos utilizando SNMP, es mejor que CDP_DP_THREAD_POOL_SIZE sea similar al número de sistemas remotos supervisados. Al definir el tamaño de agrupación similar al número de sistemas remotos supervisados, el agente recopila los datos en paralelo, pero limita la carga simultánea en los sistemas remotos. Los daemons de SNMP tienden a descartar las solicitudes cuando están ocupados. Al descartar las solicitudes se fuerza al agente a entrar en una modalidad de intentar de nuevo y que acaba por emplear más tiempo y más recursos para recopilar los datos.
- Si el agente incluye varios grupos de atributos que tardan mucho tiempo en recopilar, utilice suficientes hebras para que las recopilaciones de datos largos puedan ejecutarse en paralelo. Probablemente puede añadir unas cuantas más para el resto de los grupos de atributos. Utilice hebras de esta manera si el recurso de destino puede manejarlas. Son ejemplos de grupos de atributos que pueden tardar mucho tiempo en recopilar cuando el script se ejecuta durante mucho tiempo o cuando una consulta de JDBC tarda mucho tiempo.

La ejecución de un agente con una agrupación de hebras mayor implica que el agente utilice más memoria (sobre todo, para la pila que esta asignada a cada hebra). Sin embargo no incrementa notablemente el uso de procesador del proceso ni el tamaño del conjunto de trabajo real del proceso. El agente es más eficiente con el tamaño de la agrupación de hebras correcto para la carga de trabajo. El tamaño de la agrupación de hebras se puede ajustar para proporcionar el comportamiento deseado para un agente determinado en un entorno determinado.

Cuando se recopilan los datos, estos se colocan en la memoria caché interna. Esta memoria caché se utiliza para satisfacer solicitudes adicionales hasta que se recopilen nuevos datos. El periodo de validación para la memoria caché está controlado por CDP_DP_CACHE_TTL. De forma predeterminada, el periodo de validación está establecido en 55 segundos. Cuando un agente se ejecuta en modalidad planificada, es conveniente establecer el periodo de validez en el mismo valor que CDP_DP_REFRESH_INTERVAL. Establézcalo ligeramente mayor si la recopilación de datos puede tardar mucho tiempo. Al establecer el periodo de validación de esta forma, los datos se consideran válidos hasta la siguiente recopilación planificada.

La variable final es CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT. Esta variable sólo entra cuando CDP_DP_CACHE_TTL caduca antes de recopilar datos nuevos. Cuando la copiar en caché caduca antes de recopilar datos nuevos, el agente planifica inmediatamente otra recopilación para los datos. A continuación, espera hasta CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT segundos a que la recopilación se complete. Si la nueva recopilación se completa, la memoria caché se actualiza y se devuelven datos nuevos. Si la nueva recopilación no se completa, se devuelven los datos existentes. El agente no borra la memoria caché cuando se completa CDP_DP_CACHE_TTL para evitar que ocurra un problema que se ve con el Agente Universal. Universal Agent siempre borra la memoria caché de datos cuando finaliza el periodo de validación. Si Universal Agent borra su memoria caché de datos antes de completar la nueva

recopilación, tiene una memoria caché vacía para ese grupo de atributos y no devuelve ningún dato hasta que se complete la recopilación. La no devolución de datos es un problema cuando se están ejecutando situaciones. Cualquier situación que se ejecute tras borrar la memoria caché pero antes de completar la siguiente recopilación, no verá ningún dato y todas las situaciones que se disparen se borrarán. Como resultado, muchos sucesos se disparan y se borran simplemente porque la recopilación de datos es un poco lenta. Los agentes de Agent Builder no causan este problema. Si los datos "antiguos" provocan que una situación se dispare, normalmente los mismos datos dejan dicha situación en el mismo estado. Después de completar la siguiente recopilación, la situación obtiene los datos nuevos y se dispara o se borra en función de los datos válidos.

Grupos de atributos

Los agentes de Agent Builder incluyen dos grupos de atributos que puede utilizar para inspeccionar la operación de recopilación de datos y ajustar el agente a su entorno. Los grupos de atributos son Estado de objeto de rendimiento y Estado de agrupación de hebras. Cuando se utilizan estos grupos de atributos para ajustar el rendimiento de la recopilación de datos, los datos más útiles son los siguientes:

- Atributo `Estado de objeto de rendimiento`, `Promedio de duración de recopilación`. Este atributo le muestra cuánto tarda cada grupo de atributos en recopilar datos. A menudo un pequeño porcentaje de los grupos de atributo en un agente representa la mayoría de la utilización o el tiempo del procesador que utiliza el agente. Es posible que pueda optimizar la recopilación para uno o más de estos grupos de atributos. O puede modificar el intervalo de recopilación para uno o más grupos, si no necesita que algunos datos estén tan actualizados como otros. Para obtener más información, consulte (“Ejemplos y ajuste avanzado” en la página 1255).
- Atributo `Estado de objeto de rendimiento`, `Intervalos omitidos`. Este atributo muestra cuántas veces el agente ha intentado planificar una nueva recopilación del grupo de atributos y encontró que las recopilaciones anteriores aún están en cola, esperando a ser ejecutadas o en ejecución. En un agente con comportamiento normal este valor de atributo es cero para todos los grupos de atributos. Si este número aumenta, ajuste la recopilación de datos añadiendo hebras, alargando el intervalo entre recopilaciones u optimizando la recopilación.
- Atributo `Estado de agrupación de hebras`, `Promedio de hebras activas de agrupación de hebras`. Puede comparar este valor con el grupo de atributos Tamaño de agrupación de hebras para ver cómo se está utilizando la agrupación de hebras. La asignación de un tamaño de agrupación de hebras de 100 hebras cuando el promedio de hebras activas es 6 probablemente es un desperdicio de memoria.
- `Atributos Estado de agrupación de hebras, Promedio de espera de trabajo de agrupación de hebras y Promedio de longitud de cola de agrupación de hebras.` Estos atributos representan el tiempo que gasta una recopilación de datos común esperando en la cola para ser procesada por una hebra y el número medio de recopilaciones en la cola. Debido a la forma en que se recopilan estos datos, incluso un sistema inactivo indica que al menos un promedio de un trabajo esta en espera en la cola. Un número mayor de trabajos en espera o un tiempo de espera promedio grande indica que se están impidiendo las recopilaciones. Puede considerar la adición de hebras, alargando el intervalo entre recopilaciones u optimizando la recopilación para uno o más grupos de atributos.

Datos de sucesos

Los agentes de Agent Builder pueden exponerse a distintos tipos de datos de suceso. Algunos comportamientos son comunes a todos los datos de suceso. El agente recibe cada suceso nuevo como una fila separada de datos. Cuando se recibe una fila de datos de suceso, se envía inmediatamente a Tivoli Monitoring para su procesamiento y se añade a una memoria caché interna en el agente. Las situaciones y la recopilación histórica las realiza Tivoli Monitoring cuando cada fila se envía a Tivoli Monitoring. La memoria caché se utiliza para satisfacer las solicitudes de datos de Tivoli Enterprise Portal o SOAP. El agente puede utilizar la memoria caché para realizar la detección, el filtrado y el resumen de duplicados, si se ha definido para el grupo de atributos. El tamaño de la memoria caché de sucesos para cada grupo de atributos está definido por `CDP_PURE_EVENT_CACHE_SIZE`. Esta memoria caché contiene los últimos sucesos `CDP_PURE_EVENT_CACHE_SIZE` con los más recientes devueltos primero. Son

memorias caché separadas para cada grupo de atributos de suceso. Cuando la memoria caché de un grupo de atributos se llena, el suceso más antiguo se descarta de la lista.

El agente de Agent Builder puede exponer sucesos para:

- Entradas de registro de sucesos de Windows
- Informes o condiciones de excepción de SNMP
- Registros añadidos a los archivos de registro
- Notificaciones de MBeans JMX
- Supervisores de JMX
- Los sucesos de un proveedor API Java API o proveedor de socket.
- Grupos de atributos unidos (donde uno de los orígenes de datos es un origen de datos de sucesos).

Estos sucesos se manejan de la forma más adecuada para cada uno de los orígenes. Las condiciones de excepción e informes SNMP, notificaciones JMX y sucesos de la API Java y los proveedores de socket se reciben de forma asíncrona y se reenvían a Tivoli Monitoring inmediatamente. No hay ningún ajuste requerido para estos recopiladores. El agente se subscribe para recibir las entradas de registro de sucesos de Windows del sistema operativo mediante la API de registro de sucesos de Windows. Si el agente utiliza la API de registro de sucesos antigua, sondea el sistema en busca de nuevos sucesos con los valores de agrupación de hebras. Para los grupos de atributos unidos en los que uno de los orígenes de datos es un origen de datos de sucesos, no hay ningún ajuste para aplicar al grupo de atributos unido. Pero el grupo de atributos unido se beneficia de cualquier ajuste aplicado al grupo de origen de sucesos.

La supervisión de archivos es más complicada. El agente debe supervisar la existencia de los archivos y cuando se añaden los nuevos registros a los archivos. El agente puede configurarse para supervisar archivos utilizando patrones para el nombre del archivo o el nombre estático. Como el conjunto de archivos que coincide con los patrones puede cambiar con el paso del tiempo, el agente busca archivos nuevos o cambiados cada KUMP_DP_FILE_SWITCH_CHECK_INTERVAL segundos. Esta variable de entorno global gobierna la supervisión de archivos en una instancia de agente. Cuando el agente determina las archivos adecuados a supervisar, debe determinar cuándo los cambian archivos. En los sistemas de Windows, el agente utiliza las API del sistema operativo para escuchar estos cambios. Se informa al agente cuando los archivos se actualizan y los procesa inmediatamente. En los sistemas UNIX, el agente comprueba los cambios de archivo cada KUMP_DP_EVENT segundos. Esta variable de entorno global gobierna la supervisión de archivos en una instancia de agente. Cuando el agente advierte que un archivo ha cambiado, procesa los datos nuevos en el archivo y después espera al siguiente cambio.

Ejemplos y ajuste avanzado

Ejemplo

Las variables de entorno que se utilizan para ajustes más avanzados se definen en el nivel de agente. Las siguientes variables se establecen una vez y se aplican a todos los grupos de atributos en el agente:

- CDP_DP_CACHE_TTL
- CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT
- KUMP_DP_FILE_SWITCH_CHECK_INTERVAL
- KUMP_DP_EVENT

Puede hacer que las variables siguientes se apliquen a grupos de atributos individuales. Todavía tienen un valor global que se aplica a todos los demás grupos de atributos del agente:

- CDP_DP_REFRESH_INTERVAL
- CDP_PURE_EVENT_CACHE_SIZE

Si ha definido un agente para incluir los siguientes seis grupos de atributos:

- EventDataOne
- EventDataTwo

- EventDataThree
- SampledDataOne
- SampledDataTwo
- SampledDataThree

Puede definir las siguientes variables predeterminadas:

- `CDP_DP_CACHE_TTL=55`
- `CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT=2`
- `CDP_DP_REFRESH_INTERVAL=60`
- `CDP_PURE_EVENT_CACHE_SIZE=100`

Como resultado, todos los grupos de atributos que contengan datos muestreados (SampledDataOne, SampledDataTwo y SampledDataThree) se recopilarían cada 60 segundos. Cada uno de los grupos de atributos (EventDataOne, EventDataTwo y EventDataThree) almacenaría los últimos 100 sucesos en su memoria caché.

Estos valores podrían funcionar perfectamente, o podría necesitar controlar los valores a un nivel más granular. Por ejemplo, qué sucede si EventDataOne normalmente recibe 10 veces más sucesos que EventDataTwo y EventDataThree? Para complicar aún más las cosas, realmente existe un enlace entre EventDataOne y EventDataTwo. Cuando se recibe un suceso para EventDataTwo, siempre hay más sucesos para EventDataOne y los usuarios desean correlacionar los sucesos. No existe ni un valor correcto para el tamaño de memoria caché. Estaría bien EventDataOne pudiera almacenar un número mayor de sucesos y EventDataTwo un número inferior. Puede obtener este almacenamiento si define `CDP_PURE_EVENT_CACHE_SIZE` a un tamaño que tenga sentido para la mayoría de grupos de atributos de sucesos, 100 parece adecuado. A continuación, puede definir `CDP_EVENTDATAONE_PURE_EVENT_CACHE_SIZE` en 1000. De esta forma, todos los sucesos correspondientes están visibles en Tivoli Enterprise Portal.

Lo mismo puede llevarse a cabo con `CDP_DP_REFRESH_INTERVAL`. Establezca un valor predeterminado que funcione para el mayor número posible de grupos de atributos del agente. Después, defina `CDP_`*`nombre de grupo de atributos`*`_REFRESH_INTERVAL` para los grupos de atributo que deben recopilarse de manera distinta. Para optimizar la recopilación, defina el `CDP_DP_REFRESH_INTERVAL` predeterminado para que coincida con el valor de `CDP_DP_CACHE_TTL`. `CDP_DP_CACHE_TTL` es un valor global, por lo que si se establece en un valor menor que el intervalo de renovación, puede producir recopilaciones inesperadas.

Definición y prueba de orígenes de datos

Agent Builder soporta diversos proveedores de datos. Puede crear orígenes de datos de cada proveedor de datos. El procedimiento para crear y probar orígenes de datos es distinto para cada proveedor de datos.

Para la mayoría de proveedores de datos, al crear un origen de datos, se añade un conjunto de datos (grupo de atributos) al agente. El conjunto de datos contiene la información recopilada por este origen de datos.

Un origen de datos con un proveedor de datos Process, servicio de Windows, o Código de retorno de programa utiliza el conjunto de datos Disponibilidad especial. Solo se puede crear un conjunto de datos Disponibilidad en un agente. Contiene la información recopilada por todos los orígenes de datos con un proveedor de datos Process, servicio de Windows, o Código de retorno de programa en este agente.

Todos los orígenes de datos de registro de Windows de un agente o subnodo colocan información del suceso en un conjunto de datos de registro de sucesos.

Configuración de una fuente de datos para Cloud APM

En Cloud APM, puede utilizar los datos de todos los conjuntos de datos en el panel de instrumentos de detalles y para configurar los umbrales mediante el gestor de umbrales. Si desea utilizar la información

de un conjunto de datos en el panel de instrumentos de resumen para el agente o subnodo, incluido el indicador de estado, así como para información de recurso (nombre de servicio, dirección y puerto), el conjunto de datos debe producir solo una fila.

Para la mayoría de proveedores de datos, puede seleccionar **Produce una sola fila de datos** en la configuración de conjunto de datos. Si la información recopilada incluye más de una fila, puede pulsar **Avanzado** para configurar un filtro que asegura que se produce la fila correcta (para obtener instrucciones, consulte "Filtrado de grupo de atributos" en la página 1239). Puede probar el origen de datos para asegurarse de que la información recopilada produce la fila que necesita.

Para algunos proveedores de datos, el conjunto de datos debe producir varias filas. Además, los orígenes de datos de proceso, servicio Windows, y código de retorno de mandato colocar datos en un solo conjunto de datos de Disponibilidad, que genera varias filas. En estos casos, debe crear un conjunto de datos filtrado que genere una fila. Para obtener instrucciones sobre la creación de un conjunto de datos filtrado (grupo de atributos), consulte "Creación de un grupo de atributos filtrado" en la página 1382.

Algunos otros proveedores de datos producen datos de suceso; se incluye una fila por cada suceso nuevo. No utilice estos proveedores de datos para obtener información de resumen o de recurso en Cloud APM.

Los proveedores de datos siguientes deben producir un conjunto de datos con varias filas:

- Proceso (utiliza el conjunto de datos de Disponibilidad)
- Servicio Windows (utiliza el conjunto de datos de Disponibilidad)
- Código de retorno de programa (utiliza el conjunto de datos de Disponibilidad)
- Para algunos tipos de datos, SNMP y JMX
- En función de la aplicación, API Socket y Java

Los proveedores de datos siguientes producen los datos de suceso:

- Suceso SNMP
- Archivo de registro
- Registro binario de AIX
- Registro de sucesos de Windows
- En función de la aplicación, API Socket y Java

Uno de los atributos del conjunto de datos debe proporcionar un valor de estado. Cloud APM utiliza este valor para el indicador de estado general. Si la fila no incluye un atributo que se puede utilizar como un indicador de estado, puede crear un atributo derivado para calcular el estado. Debe configurar los valores de gravedad de estado; para obtener instrucciones, consulte "Especificar la gravedad de un atributo utilizado como indicador de estado" en la página 1238.

Supervisión de un proceso

Puede definir un origen de datos que supervisa un proceso o varios procesos que se ejecutan en un servidor. Los procesos deben ejecutarse en el mismo host que el agente. Para cada proceso, el origen de datos añade una fila al conjunto de datos de Disponibilidad.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Un proceso** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **Un proceso**.
3. Pulse **Siguiente**.
4. En la página **Supervisor de procesos**, en el área **Información de proceso**, proporcione el nombre de visualización y el nombre de proceso. Puede escribir el nombre de proceso manualmente u obtenerlo pulsando **Examinar**. Cuando se pulsa **Examinar** se muestra una lista de procesos que se ejecutan actualmente en el sistema local o en un sistema remoto.

Puede discriminar más los procesos seleccionando las opciones **Utilizar coincidencia de argumentos** y **Coincidir con línea de mandato completa**. Por ejemplo, si varias instancias de los mismos procesos se ejecutan en el sistema, se puede distinguir una instancia de otra utilizando estas opciones.

*Tabla 265. Campos de la página **Supervisor de proceso**.* Una tabla que lista los cambios en la página **Supervisor de proceso** y sus descripciones.

Nombre del campo	Descripción	Valores aceptables
Nombre de visualización	Nombre descriptivo para el componente de la aplicación que se implementa a través del proceso tal como se muestra en Tivoli Enterprise Portal o en la consola IBM Cloud Application Performance Management	Cadena descriptiva
Nombre de proceso	Nombre del proceso que está supervisándose	Nombre de archivo ejecutable válido
Utilizar coincidencia de argumento	Se selecciona si se desea la coincidencia de argumentos de proceso.	Activado o Desactivado
Argumento	Cadena de argumento que debe coincidir. La coincidencia de argumentos busca la cadena proporcionada como una subcadena de los argumentos. La coincidencia es satisfactoria si proporciona cualquier parte de los argumentos como la cadena de entrada.	Serie
Coincidencia con línea de mandatos completa	Especifique el nombre completo del archivo ejecutable que podría incluir la vía de acceso	Activado o Desactivado
Línea de mandatos	Coincide con la cadena proporcionada con el nombre de mandato completamente cualificado que se utiliza para iniciar el proceso. Los argumentos del mandato no se incluyen. Completamente cualificado significa que se debe incluir la vía de acceso del mandato.	Serie
Sistemas operativos	Seleccione los sistemas operativos en los que este proceso se ejecuta	Cualquier selección

5. Si pulsa **Examinar**, se abre la ventana **Navegador de procesos**. Esta ventana contiene inicialmente información detallada sobre cada proceso del sistema Agent Builder. La información incluye el ID, el nombre de proceso y la línea de mandatos completa para el proceso. Seleccione uno o más procesos o trabaje con la lista de la ventana **Navegador de procesos** utilizando una o varias de las acciones siguientes:
   a) Para clasificar la lista de procesos, pulse en la cabecera de columna.
   b) Para renovar la información de la ventana, pulse el icono **Renovar** (el icono del rayo).
   c) Para buscar procesos específicos, pulse el icono **Buscar** (binoculares).

Puede especificar una frase de búsqueda y seleccionar la sección de opciones para buscar por identificados de proceso, nombre y línea de mandatos.

d) Para ver procesos en un sistema diferente, seleccione un sistema definido previamente en la lista **Nombre de conexión**. O pulse **Añadir** para entrar la información del sistema para un sistema nuevo.

Para obtener más información, consulte el apartado "Definición de conexiones para examen de procesos" en la página 1260. Puede cargar procesos desde más de un sistema a la vez, y cambiar entre conexiones mientras los procesos se cargan para una o más conexiones.

Nota: Cuando examina sistemas remotos, los detalles de línea de mandatos solo están disponibles al examinar en Tivoli Enterprise Portal Server.

En el ejemplo siguiente, después de seleccionar `svchost.exe`, se muestra en el campo **Nombre de proceso** en la página **Supervisor de proceso** (Figura 31 en la página 1259).

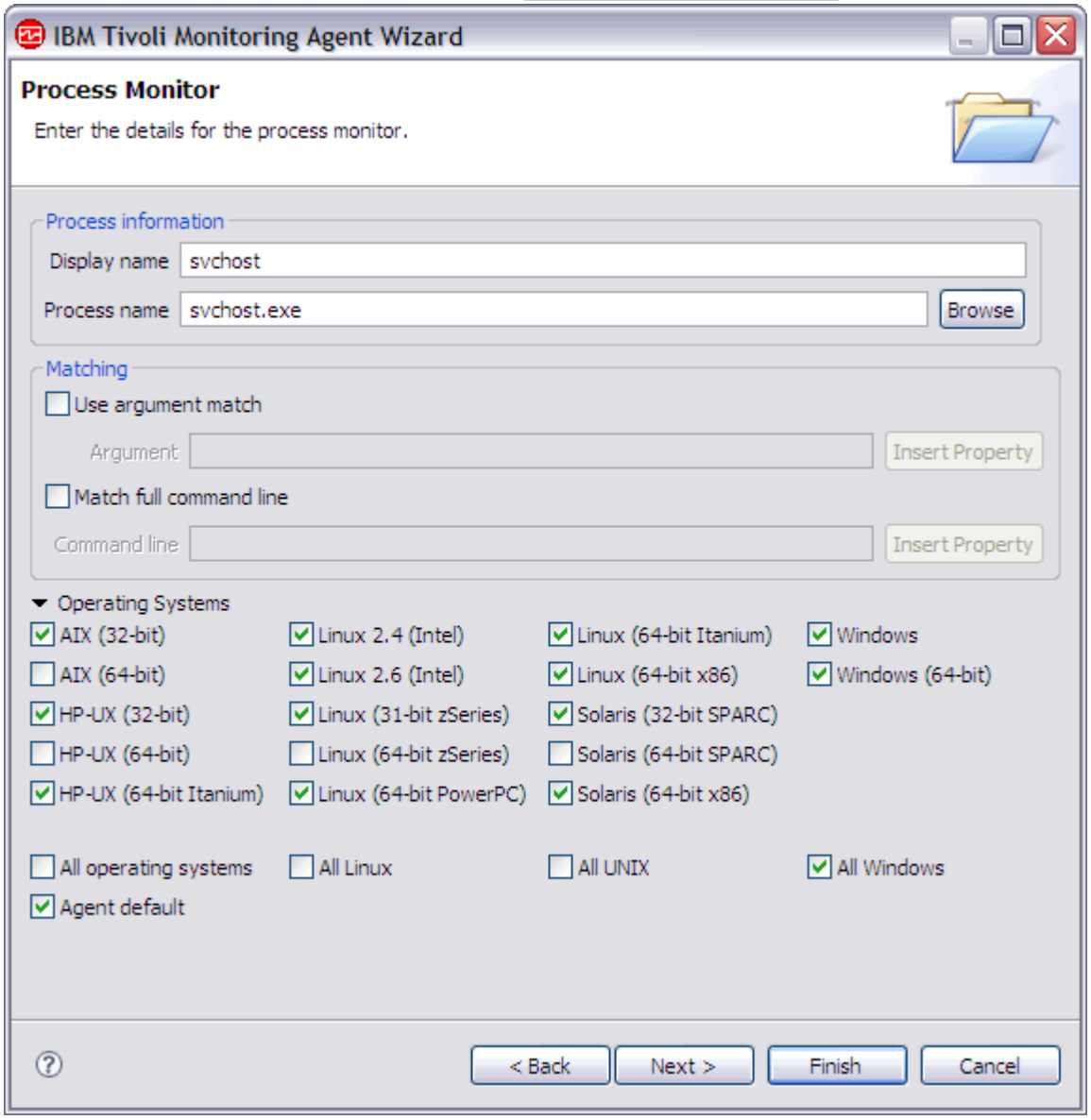


Figura 31. Ejemplo de página Supervisor de proceso

6. Complete la página **Supervisor de proceso** utilizando la información de la Tabla 265 en la página 1258.

Nota: Si el proceso que ha descrito en el supervisor es aplicable únicamente a algunos de los sistemas operativos en los que se ejecuta la aplicación, es posible que desee crear uno o más supervisores de proceso con el mismo nombre de visualización para cubrir los demás sistemas operativos. Añada los

supervisores de proceso uno cada vez. Asegúrese de que el nombre de visualización es el mismo para cada supervisor, pero que el nombre de proceso pueda encontrarse en el sistemas operativos que se han seleccionado.

7. Realice una de las acciones siguientes:
   - Si utiliza el **Asistente de agente**, pulse **Siguiente**.
   - Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.

Qué hacer a continuación

Si desea utilizar los datos de este origen de datos en el panel de instrumentos de resumen para IBM Cloud Application Performance Management, debe crear un conjunto de datos filtrados (grupo de atributos) basado en el conjunto de datos de disponibilidad y configurarlo para proporcionar una sola fila. Utilice el campo NOMBRE para seleccionar la fila para su proceso.

Puede utilizar el campo Estado para el estado; INACTIVO significa que el proceso no se está ejecutando, mientras ACTIVO significa que se está ejecutando. En el grupo de atributos filtrados nuevo, seleccione el campo Estado y especifique los valores de gravedad para él.

Si varias copias del proceso están en ejecución, varias filas con este nombre de proceso están presentes en el conjunto de datos Disponibilidad, y todos incluyen el estado ACTIVO. El conjunto de datos filtrados debe estar configurado para devolver una fila, por lo tanto, puede devolverse cualquiera de estas filas, pero el valor de Estado es válido en cualquier caso.

Para obtener instrucciones consulte:

- “Creación de un grupo de atributos filtrado” en la página 1382
- “Especificar la gravedad de un atributo utilizado como indicador de estado” en la página 1238
- “Preparación del agente para Cloud APM” en la página 1414

Definición de conexiones para examen de procesos

Al definir un origen de datos de proceso, puede ver y seleccionar procesos de otros sistemas. No obstante, cuando se ejecuta el agente, éste supervisa los procesos que se ejecutan en el mismo sistema que el agente.

Acerca de esta tarea

Debe tener credenciales para los otros sistemas o deben estar supervisados por un agente del sistema operativo de Tivoli Monitoring.

Procedimiento

1. Para definir una conexión, pulse **Añadir** en la ventana **Navegador de procesos**.

   Puede seleccionar un tipo de conexión (Secure Shell (SSH), Windows o Tivoli Enterprise Portal Server Managed System) o seleccionar una conexión existente para utilizar como plantilla.

   Para añadir una conexión de sistema gestionado, necesita un nombre de host de Tivoli Enterprise Server, un nombre de usuario de Tivoli Monitoring y una contraseña. También se necesita el nombre de sistema gestionado de la conexión remota. Cuando haya seleccionado un sistema gestionado, en la tabla aparecerá el proceso del sistema remoto.

   Nota: El agente del SO debe ejecutarse en el sistema que intente examinar. El agente debe también estar conectado a un servidor de Tivoli Enterprise Monitoring en ejecución y al servidor de Tivoli Enterprise Portal.

   Para añadir conexiones de Secure Shell (SSH) o Windows, necesita un nombre de host, un nombre de usuario y una contraseña.
2. Al añadir una conexión, puede seleccionar la conexión en la lista **Nombre de conexión** en la ventana **Navegador de procesos**.

   Si no se han guardado todos los cambios necesarios para realizar la conexión (por ejemplo, la contraseña), se abre la ventana **Propiedades de conexión** para esa conexión. Escriba la información

que falta. Para conexiones de sistema gestionado del servidor de Tivoli Enterprise Portal, debe conectarse con el servidor de Tivoli Enterprise Portal antes de poder especificar un sistema gestionado.

3. Escriba el nombre de usuario y la contraseña y, a continuación, pulse el icono **Renovar** (el icono del rayo) antes de seleccionar el sistema gestionado.

Qué hacer a continuación

Para eliminar una conexión, seleccione la conexión y pulse **Editar** para abrir la ventana **Propiedades de conexión**. Seleccione el recuadro de selección **Eliminar esta conexión** y pulse **Aceptar**.

Supervisión de un servicio de Windows

Puede definir un origen de datos que supervisa un servicio o varios servicios que se ejecutan en un sistema Windows. Los servicios se deben ejecutar en el mismo host que el agente. Para cada servicio, el origen de datos añade una fila al conjunto de datos Disponibilidad.

Procedimiento

1. En la página **Origen de datos inicial de agente** o la página **Ubicación de origen de datos**, pulse **Un proceso** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse en **Un servicio de Windows**.
3. Pulse **Siguiente**.
4. En la página **Supervisor de servicio**, en el campo **Nombre de visualización**, escriba una descripción. En el campo **Nombre de servicio**, proporcione el nombre de la aplicación de servicio. Puede escribirlo manualmente o pulsar **Examinar** para ver una lista de servicios que se ejecutan actualmente en el sistema local o en un sistema remoto.

   Si pulsa **Examinar**, se abre la ventana **Navegador de servicios**. Esta ventana contiene inicialmente información detallada sobre cada servicio del sistema Agent Builder. La información incluye el nombre de servicio, el nombre de visualización, el estado y la descripción para el servicio.

   Nota: Los servicios locales no se muestran cuando Agent Builder no se ejecuta en un sistema Windows. Debe estar definido o seleccionado un sistema Windows remoto, consulte ("Definición de conexiones para examen de servicios" en la página 1262).

   Nota: La descripción de servicio no está disponible cuando se examina a través del servidor de Tivoli Enterprise Portal o desde un sistema UNIX o Linux.
5. Seleccione uno o varios servicios o siga uno o más de los pasos siguientes para trabajar con la lista en la ventana **Navegador de servicios**¡:
   - Para ordenar la lista de servicios, pulse la cabecera de columna.
   - Para renovar la información de la ventana, pulse el icono **Renovar** (el icono del rayo).
   - Para buscar un servicio, pulse el icono **Búsqueda** (binoculares) para abrir la ventana **Búsqueda de servicio**. Puede buscar por el nombre de servicio, el nombre de visualización y la descripción.
   - Para ver servicios en un sistema diferente, seleccione un sistema previamente definido en la lista **Nombre de conexión** o pulse **Añadir** para especificar la información de sistema. Para obtener más información, consulte ("Definición de conexiones para examen de servicios" en la página 1262). Puede cargar servicios desde más de un sistema a la vez, y cambiar entre conexiones mientras los servicios se cargan para una o más conexiones.
6. Tras seleccionar o especificar el nombre del servicio, complete uno de los pasos siguientes:
   - Si utiliza el **Asistente de agente**, pulse **Siguiente**.
   - Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.

Qué hacer a continuación

Si desea utilizar los datos de este origen de datos en el panel de instrumentos de resumen para IBM Cloud Application Performance Management, debe crear un conjunto de datos filtrados (grupo de

atributos) basado en el conjunto de datos de disponibilidad y configurarlo para proporcionar una sola fila. Utilice el campo NOMBRE para seleccionar la fila para su proceso.

En el grupo de atributos filtrados nuevo, seleccione el campo Estatus_prueba_funcionalidad y especifique los valores de gravedad para él.

Para obtener instrucciones consulte:

- “Creación de un grupo de atributos filtrado” en la página 1382
- “Especificar la gravedad de un atributo utilizado como indicador de estado” en la página 1238
- “Preparación del agente para Cloud APM” en la página 1414

Definición de conexiones para examen de servicios
Además de seleccionar servicios del sistema en el que Agent Builder se ejecuta, puede seleccionar servicios de otros sistemas Windows.

Acerca de esta tarea

Para seleccionar servicios de otros sistemas Windows, defina una conexión con el sistema remoto. Debe tener credenciales para los sistemas o estos deben estar supervisados por un agente del sistema operativo Tivoli Monitoring.

Procedimiento

1. Para definir una conexión, pulse **Añadir** en la ventana **Navegador de servicios**.

   Se abre la ventana **Seleccionar tipo de conexión**. Para añadir una conexión de sistema gestionado, se necesita un nombre de host de Tivoli Enterprise Server, un nombre de usuario y contraseña de Tivoli Monitoring y el nombre de sistema gestionado. Cuando haya seleccionado un sistema gestionado, en la tabla aparecerá el servicio del sistema remoto.

   Nota: El agente de SO se debe estar ejecutando en el sistema que intenta examinar y también debe estar conectado a un Tivoli Enterprise Monitoring Server y a un Tivoli Enterprise Portal Server en ejecución.

   Necesita un nombre de host, un nombre de usuario y una contraseña para añadir una conexión Windows.
2. Seleccione un tipo de conexión (Windows, o Tivoli Enterprise Portal Server Managed System) o seleccione una conexión existente para utilizar como plantilla.

   Se abre la ventana **Propiedades de conexión**.
3. Complete las propiedades de conexión.
4. Pulse **Finalizar**
5. Al añadir una conexión, puede seleccionar la conexión en la lista **Nombre de conexión** en la ventana **Navegador de servicios**.

   Si no se han guardado los campos necesarios para realizar la conexión (por ejemplo, la contraseña), se abre la ventana **Propiedades de conexión** y puede entrar la información que falta.

   a) Para las conexiones de sistema gestionado de Tivoli Enterprise Portal Server, debe conectarse a Tivoli Enterprise Portal Server antes de poder entrar un sistema gestionado. Escriba el nombre de usuario y la contraseña y, a continuación, pulse el icono **Renovar** (el icono del rayo) antes de seleccionar el sistema gestionado.
6. Para suprimir una conexión, siga estos pasos:

   a) Seleccione la conexión en la ventana **Navegador de servicios**.

   b) Pulse **Editar** para abrir la ventana **Propiedades de conexión**.

   c) Marque el recuadro de selección **Eliminar esta conexión**.

   d) Pulse **Aceptar**.

Supervisión de datos de Windows Management Instrumentation (WMI)

Puede definir un origen de datos para recopilar datos de Windows Management Instrumentation (WMI) en el sistema donde se ejecuta el agente o en un sistema remoto. Un origen de datos supervisa una sola clase WMI y coloca todos los valores de esta clase en el conjunto de datos que se genera. Si la clase proporciona varias instancias, el conjunto de datos tiene varias filas; puede filtrar por nombre de instancia para asegurarse de que el conjunto de datos tiene una fila.

Antes de empezar

Si el agente recopila datos de un sistema remoto utilizando Windows Management Instrumentation (WMI), necesita permisos para acceder a datos WMI en el sistema remoto. El agente puede acceder a datos WMI de un sistema remoto cuando se proporcionan credenciales de una cuenta con permisos para acceder a datos WMI del sistema. La cuenta de administrador tiene los permisos necesarios. En el procedimiento siguiente, puede proporcionar las credenciales de administrador o las credenciales de otro usuario con los permisos necesarios. Si desea más información sobre cómo crear una cuenta de usuario con permisos para examinar datos de WMI, consulte "Creación de un usuario con permisos de Windows Management Instrumentation (WMI)" en la página 1405.

Para recopilar medidas mediante las API de Windows, el agente debe estar alojado en un sistema operativo Windows. La administración de registro remota debe estar habilitada en los sistemas remotos.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos de un servidor** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **WMI**.
3. Pulse **Siguiente**.
4. En la página **Información de Windows Management Instrumentation (WMI)**, complete uno de los pasos siguientes:
   - Escriba un nombre para el espacio de nombres de WMI y un nombre para el nombre de clase WMI en los campos. A continuación, vaya al paso "9" en la página 1263
   - Pulse **Examinar** para ver todas las clases WMI del sistema.

     Para examinar un sistema remoto, seleccione un sistema en la lista (si hay alguno definido). De forma alternativa, pulse **Añadir** para añadir el nombre de host de un sistema Windows. Proporcione las credenciales de una cuenta de usuario con permisos para acceder a datos WMI en el sistema remoto, o proporcione credenciales de administrador para el sistema remoto. La página se actualiza con la información para el sistema remoto. El examen solo está disponible cuando Agent Builder se ejecuta en un sistema Windows y solo puede examinar sistemas Windows.

5. Pulse el signo más (+) situado junto a una clase para expandir la clase y mostrar los atributos.
6. Desde la lista, seleccione la clase con sus atributos asociados que desea especificar y pulse **Aceptar**.

   Nota: Puede pulsar en el icono **Buscar** (binoculares) para buscar la selección en la lista. Escriba una frase en el campo **Frase de búsqueda**; especifique sus preferencias pulsando **Buscar por nombre**, **Buscar por descripción de clase** o **Buscar por propiedades de clase** y pulse **Aceptar**. Si encuentra el elemento que está buscando, selecciónelo y pulse **Aceptar**.

   Se vuelve a abrir la página **Información de WMI** del asistente mostrando la información de clase WMI seleccionada.
7. Opcional: Puede probar este grupo de atributos pulsando **Probar**. Para obtener más información sobre la prueba, consulte "Prueba de grupos de atributos de WMI" en la página 1264
8. Opcional: Puede crear un filtro para limitar los datos que este grupo de atributos devuelve pulsando **Avanzado**. Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte "Filtrado de grupo de atributos" en la página 1239
9. Pulse **Siguiente**.

Nota: Si ha escrito el nombre de clase y el espacio de nombres de WMI manualmente, se abrirá la página **Información de atributos**, donde puede completar la información de atributo. En la página **Información de atributos**, puede seleccionar **Añadir atributos adicionales** si desea añadir más atributos. Pulse **Finalizar** para terminar.

10. En la página **Seleccionar atributos clave**, seleccione los atributos clave o indique que este origen de datos solo produce una fila de datos. Para obtener más información, consulte ("Selección de atributos clave" en la página 1208).
11. Realice una de las acciones siguientes:
    - Si utiliza el **Asistente de agente**, pulse **Siguiente**.
    - Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.
12. Es posible añadir atributos y proporcionar la información para los mismos. Para obtener más información, consulte el apartado "Creación de atributos" en la página 1230.

    Además de los campos aplicables a todos los orígenes de datos (Tabla 261 en la página 1234), la página **Información de atributos** para el origen de datos WMI tiene el campo siguiente:

    Nombre de medida
    Nombre de propiedad de la clase que se desea recopilar
13. Si desea establecer opciones globales para el origen de datos, pulse **Opciones globales**.

    Seleccione el recuadro de selección **Incluir propiedades de configuración de Windows remoto** si desea incluir esta opción y pulse **Aceptar**.

    Para obtener información sobre la configuración de conexión remota de Windows para orígenes de datos de Windows, consulte "Configuración de una conexión remota de Windows" en la página 1404.

Prueba de grupos de atributos de WMI
Si está ejecutando Agent Builder en un sistema Windows, podrá probar un grupo de atributos WMI en Agent Builder.

Procedimiento

1. El procedimiento de prueba se puede iniciar de las siguientes formas:
    - Durante la creación del agente, pulse **Probar** en la página **Información de WMI**.
    - Después de la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** de Agent Editor y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208.

    Después de pulsar **Probar** en uno de los dos pasos anteriores, se muestra la ventana **Prueba de WMI**.
2. Opcional: Antes de empezar la prueba, puede establecer variables de entorno y propiedades de configuración. Para obtener más información, consulte "Prueba de grupo de atributos" en la página 1417.
3. Pulse **Iniciar agente**.

    Una ventana indica que el agente se está iniciando.
4. Para simular una solicitud de entorno de supervisión de datos del agente, pulse **Recopilar datos**.

    El agente consulta los datos en WMI. La ventana **Prueba de WMI** recopila y muestra los datos de la memoria caché del agente desde que se inició por última vez.
5. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

    Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana **Estado de la recopilación de datos** recopila y muestra se describen en ("Nodo Estatus de objeto de rendimiento" en la página 1462).
6. Detenga el agente pulsando **Detener agente**.
7. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Prueba de WMI**. Al pulsar **Aceptar** se guardan los cambios que ha realizado.

Conceptos relacionados

"Pruebas del agente en Agent Builder" en la página 1417
Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión del Windows Performance Monitor (Perfmon)

Puede definir un origen de datos para recopilar datos de Windows Performance Monitor (Perfmon). Un origen de datos supervisa un objeto Perfmon. Los contadores del objeto se colocan en atributos en el conjunto de datos resultante. Si la clase proporciona varias instancias, el conjunto de datos tiene varias filas; puede filtrar por nombre de instancia para asegurarse de que el conjunto de datos tiene una fila.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos de un servidor** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **Perfmon**.
3. Pulse **Siguiente**.
4. En la página **Información de Perfmon**, complete uno de los pasos siguientes:
   - Escriba el nombre del objeto en el campo **Nombre de objeto** y pulse **Siguiente** para definir el primer atributo del grupo de atributos.

     Nota: Si escribe el nombre para el objeto de Windows Performance Monitor, debe ser en inglés.
   - Pulse **Examinar** para ver la lista de objetos de Perfmon.

     Cuando la ventana del navegador del objeto Supervisor de rendimiento (Perfmon) se abre inicialmente, la ventana se llena con información del sistema local. Para examinar un sistema remoto, seleccione un sistema de la lista (si hay alguno definido), o pulse **Añadir** para añadir el nombre de host de un sistema Windows. Proporcione un ID y una contraseña de administrador. La ventana se actualiza con la información correspondiente al sistema remoto. Solo se puede examinar si el Agent Builder se está ejecutando en un sistema Windows y puede examinar solo sistemas Windows. Por ejemplo, no puede añadir el nombre de host de un sistema Linux o Solaris para realizar un examen remoto.

     – Al pulsar un nombre de objeto, los contadores disponibles en dicho objeto se muestran en la ventana.

       - Para ordenar los objetos o los contadores del Windows Performance Monitor, pulse la cabecera de la columna.
       - Para renovar la información de la ventana, pulse en **Renovar**.
       - Para buscar objetos o contadores específicos, pulse el icono **Buscar** (binoculares) para abrir la ventana **Búsqueda de supervisor de rendimiento**. Puede buscar nombres de objeto, nombres de contadores o ambos. La operación de búsqueda realiza una coincidencia de subcadenas y no distingue entre mayúsculas y minúsculas.
       - Seleccione un objeto y pulse **Aceptar**.
       - Se abre la página **Información de Perfmon** con el nombre del objeto seleccionado en el campo **Nombre de objeto**.
   - Si desea establecer opciones globales para la fuente de datos, pulse **Opciones globales**

     Seleccione el recuadro de selección **Incluir propiedades de configuración de Windows remoto** si desea incluir esta opción y pulse **Aceptar**.

     Para obtener información sobre la configuración de conexión remota de Windows para orígenes de datos de Windows, consulte "Configuración de una conexión remota de Windows" en la página 1404.
5. Si el objeto de Windows Performance Monitor seleccionado devuelve varias instancias y desea filtrar los resultados que están basados en el nombre de instancia:

a) Seleccione el recuadro de selección **Filtrar por nombre de instancia de Perfmon** en la página **Información de Perfmon**.

b) En el campo **Nombre de instancia de Perfmon**, escriba el nombre de la instancia que debe filtrarse o pulse **Examinar** para listar las instancias disponibles.

c) Para examinar un sistema remoto, seleccione uno en la lista, o pulse **Añadir** para añadir el nombre de host de un sistema Windows. Después de seleccionar un host, proporcione un ID y una contraseña de administrador. La tabla se actualiza con la lista de instancias del sistema remoto.

Nota: También puede filtrar por grupo de atributos, consulte el paso "9" en la página 1266

6. Si el objeto de Windows Performance Monitor seleccionado va a devolver varias instancias, y desea que se devuelva el nombre de instancia, seleccione **Devolver nombre de instancia** en la página **Información de Perfmon**.

   Cuando se selecciona esta opción, se añade un atributo al origen de datos que no se muestra en la lista de atributos. Este atributo contiene el nombre de la instancia.

   Nota: Si ha examinado el objeto seleccionado y dicho objeto está definido como propietario de varias instancias, este recuadro de selección se selecciona de forma automática.

7. Si no ha seleccionado la opción para devolver el nombre de instancia, se abre la página Seleccionar atributos clave. En la página Seleccionar atributos clave, seleccione atributos clave o indique que este origen de datos solo genera una fila de datos. Para obtener más información, consulte ("Selección de atributos clave" en la página 1208).
8. Opcional: Puede probar este grupo de atributos pulsando **Probar**. Para obtener más información sobre la prueba, consulte "Prueba de grupos de atributos de Perfmon" en la página 1266
9. Opcional: Puede crear un filtro para limitar los datos que este grupo de atributos devuelve pulsando **Avanzado**.

   Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte el paso "Filtrado de grupo de atributos" en la página 1239

   Nota: También puede filtrar por nombre de instancia, consulte "5" en la página 1265

10. Realice una de las acciones siguientes:

    - Si utiliza el Asistente de agente nuevo, pulse **Siguiente**.
    - Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.

      La página **Definición de origen de datos** de **Agent Editor** muestra una lista que contiene el objeto y la información sobre el objeto.

11. Es posible añadir atributos y proporcionar la información para los mismos. Para obtener más información, consulte ("Creación de atributos" en la página 1230).

    Además de los campos aplicables a todos los orígenes de datos, la página **Información de atributos de Perfmon** para el origen de datos tiene el campo siguiente:

    Nombre de medida
    Nombre del contador para el objeto específico.

Qué hacer a continuación

Si desea información sobre la configuración de conexión remota de Windows para orígenes de datos de Perfmon, consulte "Configuración de una conexión remota de Windows" en la página 1404.

Prueba de grupos de atributos de Perfmon

Si está ejecutando el Agent Builder en un sistema Windows, puede probar el grupo de atributos de rendimiento que ha creado.

Procedimiento

1. El procedimiento de prueba se puede iniciar de las siguientes formas:

   - Durante la creación del agente, pulse **Probar** en la página **Información de Perfmon**.

- Tras la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** del Agent Editor y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte “Utilización del editor del agente para modificar el agente” en la página 1208.

Tras pulsar **Probar** en uno de los dos pasos anteriores, se muestra la ventana **Prueba de Perfmon**.

2. Opcional: Antes de empezar la prueba, puede establecer variables de entorno y propiedades de configuración. Para obtener más información, consulte “Prueba de grupo de atributos” en la página 1417.
3. Pulse **Iniciar agente**. Una ventana indica que el agente se está iniciando.
4. Para simular una solicitud desde el entorno de supervisión para los datos de agente, pulse **Recopilar datos**.

   El agente consulta los datos en el supervisor de rendimiento. La ventana **Prueba de Perfmon** recopila y muestra los datos de la memoria caché del agente desde que se inició por última vez.

   Nota: Puede que no vea datos útiles para todos los atributos hasta que pulse **Recopilar datos** por segunda vez. La razón es que algunos atributos del Monitor de rendimiento devuelven valores delta, y se necesita un valor anterior para calcular un valor delta.
5. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana **Estado de la recopilación de datos** recopila y muestra se describen en “Nodo Estatus de objeto de rendimiento” en la página 1462.
6. Detenga el agente pulsando **Detener agente**.
7. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Prueba de Perfmon**. Al pulsar **Aceptar** se guardan los cambios que ha realizado.

Conceptos relacionados

“Pruebas del agente en Agent Builder” en la página 1417
Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión de datos procedentes de un servidor de protocolo simple de gestión de red (SNMP)

Puede definir un origen de datos para supervisar un servidor SNMP. Un origen de datos supervisa todos los datos de un único identificador de objeto (OID) SNMP y un solo host. Si selecciona un elemento del árbol de registro de identificadores de objeto bajo el que están registrados otros objetos, se creará un conjunto de datos para cada conjunto distinto de valores escalares o de tabla. Si un objeto devuelve datos escalares, el conjunto de datos tendrá una sola fila. Si un objeto devuelve datos tabulares, el conjunto de datos tendrá varias filas.

Acerca de esta tarea

Simple Network Management Protocol V1, V2C (observe que la versión es V2C y no sólo V2) y V3 son soportados por los agentes.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos de un servidor** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **SNMP**.
3. Pulse **Siguiente**.
4. En la página Información de SNMP (Simple Network Management Protocol), escriba el nombre de visualización o pulse **Examinar** para ver todos los objetos del sistema.

   Después de definir el origen de datos, puede añadir un atributo. Los OID de estos atributos pueden ser largos y difíciles de escribir correctamente. Utilizar la opción de búsqueda es una forma sencilla de introducir el OID correcto.

Nota: El navegador no examina el sistema activo, lee las definiciones y las MIB (bases de información de gestión).

Nota: Al pulsar en el icono de **Renovar** se borra la versión en memoria de los archivos MIB analizados y se vuelven a analizar los archivos en la memoria caché del espacio de trabajo. La memoria caché de la siguiente ubicación: *directorio_espacio_trabajo*\.metadata \.plugins\ com.ibm.tivoli.monitoring.agentkit\mibs

Donde:

directorio_espacio_trabajo
Identifica el directorio de espacio de trabajo que ha especificado cuando ha ejecutado inicialmente Agent Builder, consulte ("Inicio de Agent Builder" en la página 1203).

a) Si la MIB que define el objeto deseado no está cargada, pulse **Gestionar MIB personalizadas** para abrir el diálogo Gestionar MIB personalizadas.

b) Pulse en **Añadir** para examinar en el archivo MIB a añadir. Para suprimir una MIB de la memoria caché, selecciónela y pulse **Eliminar**.

c) Pulse **Aceptar** para actualizar la memoria caché.

Si hay algún error al analizar las MIB, el diálogo Gestionar MIB personalizadas permanece abierto. Este diálogo ofrece la oportunidad de añadir o eliminar las MIB para eliminar los diálogos.

Al pulsar **Cancelar**, la memoria caché de la MIB vuelve al estado en que estaba cuando se ha abierto el diálogo.

Agent Builder incluye un conjunto de MIB:

- hostmib.mib
- rfc1213.mib
- rfc1243.mib
- rfc1253.mib
- rfc1271.mib
- rfc1286.mib
- rfc1289.mib
- rfc1315.mib
- rfc1316.mib
- rfc1381.mib
- rfc1382.mib
- rfc1443.mib
- rfc1461.mib
- rfc1471.mib
- rfc1493.mib
- rfc1512.mib
- rfc1513.mib
- rfc1516.mib
- rfc1525.mib
- rfc1573a.mib
- rfc1595.mib
- rfc1650.mib
- rfc1657.mib
- rfc1659.mib
- rfc1666.mib

- rfc1695.mib
- rfc1747.mib
- rfc1748.mib
- rfc1757.mib
- rfc1903.mib
- rfc1907.mib
- rfc2011.mib
- rfc2021.mib
- rfc2024.mib
- rfc2051.mib
- rfc2127.mib
- rfc2128.mib
- rfc2155.mib
- rfc2206.mib
- rfc2213.mib
- rfc2232.mib
- rfc2233.mib
- rfc2238.mib
- rfc2239.mib
- rfc2320.mib
- rfc3411.mib

Todas estas MIB son MIB estándar, definidas por IETF. Las MIB se incluyen porque representan definiciones comunes que pueden ser útiles en la supervisión. Además, muchas de las MIB son necesarias para que las MIB personalizadas puedan resolver los símbolos que importan.

d) Seleccione un objeto de la lista.

Pulse el signo más (+) situado junto a un objeto para expandir y mostrar los niveles.

e) En la lista, seleccione el objeto que desea especificar y pulse **Aceptar**.

A continuación, el nuevo origen de datos se lista en la página **Definición de origen de datos**.

Nota: Si selecciona un objeto que define otros objetos (objetos que están anidados debajo del primer objeto), todos estos objetos se convierten en orígenes de datos. Si selecciona un objeto de nivel superior, se añaden muchos orígenes de datos.

5. En la página **Información de SNMP (Simple Network Management Protocol)**, seleccione los sistemas operativos.
6. Opcional: Puede probar el origen o los orígenes e datos pulsando **Probar** en la página **Información de SNMP (Simple Network Management Protocol)**.

   Para obtener más información sobre la prueba, consulte “Prueba de grupos de atributos SNMP” en la página 1271
7. Opcional: Puede crear un filtro para limitar los datos que este grupo de atributos devuelve pulsando **Avanzado**. Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte “Filtrado de grupo de atributos” en la página 1239
8. Pulse **Siguiente**.
9. En la página **Información de atributos**, especifique la información para el atributo.
10. Realice una de las acciones siguientes:
    - Si utiliza el Asistente de agente nuevo, pulse **Siguiente**.
    - Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.

11. Si desea más información sobre cómo añadir atributos y proporcionar la información para los mismos, consulte "Creación de atributos" en la página 1230.

    Además de los campos que se pueden aplicar a todos los orígenes de datos, la página **Información de atributos** para el origen de datos de SNMP tiene los campos siguientes:

    Nombre de medida
    Serie arbitraria

    Identificador de objeto
    OID completo registrado para el objeto, sin incluir los valores de índice

Qué hacer a continuación

Puede utilizar la configuración de tiempo de ejecución del agente para establecer el host supervisado.

Para permitir que el Agent Builder genere tipos de datos de 64-bits y para manejar el valor máximo para propiedades MIB no firmadas de 32-bits, consulte "Opciones de análisis de MIB de SNMP" en la página 1270.

Errores de MIB de SNMP
Manejo de errores en las MIB de SNMP

No es inusual encontrar errores cuando se añaden MIB de SNMP. Pulse **Detalles>>** en la ventana **Error de Agent Builder** para ver cuál es el error de MIB.

Uno de los errores más comunes es que falten definiciones que están especificadas en otros MIB. Puede importar varias MIB simultáneamente para resolver este problema, o puede ir añadiendo MIB de forma incremental hasta que se resuelvan todas las definiciones que faltan. Agent Builder puede utilizar cualquier definición que se haya resuelto. Por lo tanto, puede elegir ignorar un error que solo afecta a la parte de la MIB que no tiene previsto utilizar. El orden de las MIB no importa puesto que todos están cargados, por lo que las referencias se resuelven.

Opciones de análisis de MIB de SNMP
Establezca sus preferencias para el análisis de MIB de SNMP

Procedimiento

1. En Agent Builder, seleccione **Ventana** > **Preferencias** para abrir la ventana **Preferencias**.
2. En el panel de navegación, expanda **IBM Tivoli Monitoring Agent Builder**.
3. Pulse **Análisis de MIB** para abrir la ventana **Análisis de MIB**.

   El analizador MIB que utiliza el Agent Builder utiliza la gramática definida mediante ASN.1 para analizar las MIB. Algunas MIB no siguen la gramática correctamente. El analizador puede pasar por alto ciertas reglas para omitir los errores más comunes. Al relajar estas reglas, puede analizar las MIB no conformes.

   Permitir que los tipos empiecen con letras minúscula
   Permite los tipos que los usuarios escriben en MIB, como por ejemplo valores

   Permitir números con nombres numéricos
   Permite números que comienzan con letras mayúsculas

   Permitir signo de subrayado en nombre de valor
   Permite los caracteres de signo de subrayado

   Permitir que los valores empiecen con letras mayúsculas
   Permite valores que comienzan con letras minúsculas

   Pasar por alto MIB duplicadas
   Desactiva el aviso para módulos de MIB duplicadas
4. Opcional: Si se marca el recuadro de selección **Crear atributos de 64 bits para propiedades MIB sin signo de 32 bits**, se permite que Agent Builder genere tipos de datos de 64 bits para manejar el valor máximo para propiedades MIB sin signo de 32 bits. El hecho de seleccionar esta opción no modifica

ninguna de las definiciones de campos de agente existentes. Debe examinar el archivo MIB para crear nuevos orígenes de datos para estas propiedades.

5. Cuando haya terminado de editar las preferencias, pulse **Aceptar**.

Prueba de grupos de atributos SNMP

Puede probar el grupo de atributos SNMP que ha creado dentro de Agent Builder.

Procedimiento

1. El procedimiento de prueba se puede iniciar de las siguientes formas:
   - Durante la creación del agente, pulse **Probar** en la página **Información de Simple Network Management Protocol**.

     Nota:

     Si el objeto SNMP seleccionado contiene más de un grupo de atributos, se le pedirá que seleccione el grupo de atributos para probar.
   - Después de la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** de **Agent Editor** y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208

   Después de pulsar **Probar** en uno de los dos pasos anteriores, se abre la ventana de valores de prueba SNMP.
2. Seleccione una conexión existente en **Nombre de conexión** o pulse **Añadir** y se le solicitará que seleccione un tipo de conexión. De forma alternativa, seleccione una conexión existente para utilizarla como plantilla, utilizando el **Asistente para crear conexión**.
3. Después de seleccionar un tipo de conexión o una conexión existente, pulse **Siguiente** para completar las propiedades de conexión SNMP. Una vez completadas, pulse **Finalizar** para volver a la ventana de valores de prueba SNMP.
4. Opcional: Antes de empezar la prueba, puede establecer variables de entorno y propiedades de configuración. Para obtener más información, consulte ("Prueba de grupo de atributos" en la página 1417).
5. Pulse **Iniciar agente**. Una ventana indica que el agente se está iniciando.
6. Para simular una solicitud de Tivoli Enterprise Portal o SOAP para los datos de agente, pulse **Recopilar datos**. El agente consulta los datos en la conexión SNMP configurada.
7. La ventana **Probar valores** recopila y muestra los datos de la memoria caché del agente desde que se inició por última vez.
8. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana **Estado de la recopilación de datos** recopila y muestra se describen en "Nodo Estatus de objeto de rendimiento" en la página 1462
9. Detenga el agente pulsando **Detener agente**.
10. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Probar valores**. Al pulsar **Aceptar** se guardan los cambios que ha realizado.

Conceptos relacionados

"Pruebas del agente en Agent Builder" en la página 1417

Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión de sucesos procedentes de remitentes de sucesos SNMP (protocolo simple de gestión de red)

Puede definir un origen de datos para recopilar datos de sucesos de Informes o condiciones de excepción de SNMP. Debe establecer el puerto en la configuración de tiempo de ejecución del agente y configurar los servidores para enviar el suceso al sistema principal de agente en este puerto. Todos los sucesos supervisados se colocan como filas en un conjunto de datos.

Acerca de esta tarea

Simple Network Management Protocol (SNMP) V1, V2C (tenga en cuenta que el nombre de esta versión es V2C y no solo V2) y V3 son compatibles con agentes. El agente puede recibir y procesar las condiciones de excepción e informaciones de SNMP. Los datos recibidos por este proveedor se pasan al entorno de supervisión como sucesos.

Para obtener más información sobre los grupos de atributos para sucesos SNMP, consulte ("Grupos de atributos de sucesos SNMP" en la página 1489).

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos de un servidor** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **Sucesos de SNMP**.
3. Pulse **Siguiente**.
4. En la ventana **Información de sucesos Simple Network Management Protocol**, realice una de las acciones siguientes:
   - Pulse **Todos los sucesos** para crear un grupo de atributos que envíe un suceso para cualquier suceso de SNMP recibido.
   - Pulse **Sucesos genéricos** para crear un grupo de atributos que envíe un suceso para cualquier suceso de SNMP genérico recibido que coincida con alguno de los tipos de suceso genérico seleccionados.
   - Pulse **Sucesos personalizados** para crear uno o más grupos de atributos que envíen sucesos para sucesos de SNMP específicos de Enterprise. Pulse **Examinar** para seleccionar los sucesos que se van a supervisar.

     En la ventana **Navegador de MIB (Management Information Base) de SNMP (Simple Network Management Protocol)**, los sucesos del panel de selección se organizan por el módulo de MIB en el que se han definido. Expanda un objeto SNMP para mostrar los sucesos de ese módulo MIB. En la lista, pulse el objeto que desea especificar y pulse **Aceptar**.

     Seleccione el recuadro de selección **Incluir atributos que muestren información definida en el archivo de configuración de condiciones de excepción** si tiene un archivo de configuración de condiciones de excepción que contenga datos estáticos para las condiciones de excepción. Para obtener más información sobre el archivo de configuración de condiciones de excepción de SNMP, consulte ("Configuración de condiciones de excepción de SNMP" en la página 1543).

     Seleccione el recuadro de selección **Incluir atributo de datos de enlace de variables (VarBind)** si desea incluir un atributo con todos los datos de enlace de variables (VarBind) que se reciben en la unidad de datos de protocolo (PDU) de condición de excepción. Para obtener más información sobre este atributo, consulte la definición del atributo en "Grupos de atributos de sucesos SNMP" en la página 1489.

     Nota:

     a. El navegador no examina el sistema activo; lee las definiciones y las MIB (bases de información de gestión). La lista de MIB incluidas con el Agent Builder se define en "Supervisión de datos procedentes de un servidor de protocolo simple de gestión de red (SNMP)" en la página 1267. Las MIB cargadas por alguno de los proveedores de datos SNMP están disponibles en ambos.

     b. Si selecciona un módulo MIB o un suceso individual, todos los sucesos del módulo se convertirán en orígenes de datos independientes. Se añade un atributo a cada una de las variables que se definen en el suceso. Si desea que todos los sucesos del módulo seleccionado o las condiciones de excepción lleguen en un único origen de suceso, seleccione el recuadro de selección **Recopilar sucesos en un solo grupo de atributos**. Si selecciona condiciones de excepción individuales y el distintivo **Recopilar sucesos en un único grupo de atributos** está seleccionado, se añade un atributo para cada una de las variables que se definen en cada uno de los sucesos (las variables duplicadas se ignoran). Si selecciona un módulo, los atributos de variables no se añaden.

c. Si desea especificar su propio filtro, utilice la siguiente sintaxis:

   El valor del elemento de identificador de objeto (OID) se utiliza para determinar qué condiciones de excepción procesar para este grupo de atributos.

   – **Coincidencia de condiciones de excepción:** El atributo OID del elemento global_snmp_event_settings_for_group puede ser una lista delimitada por comas de las señales. Una única señal tiene la siguiente sintaxis:

     ```
     [enterpriseOID][-specificType]
     ```

   – **Ejemplo:** "1.2.3.5.1.4,1.2.3.4.5.6.7.8.9-0" La primera señal coincide con alguna condición de excepción con un OID de Enterprise de 1.2.3.5.1.4. La segunda señal coincide con alguna condición de excepción con una Enterprise de 1.2.3.4.5.6.7.8.9 y específica de 0. Como las señales se enumeran juntas en un grupo de atributos, un suceso recibido que coincida con alguno será procesado por dicho grupo de atributos.

d. Cada suceso que se reciba es procesado únicamente por el primer grupo de atributos que coincida con el suceso recibido. Los grupos de atributos de subnodo se procesan primero y, a continuación, los grupos de atributos básicos. El desarrollador del agente debe asegurarse de que los grupos estén definidos de forma que los sucesos se reciban en el grupo de atributos esperado.

5. En la ventana **Información de sucesos de SNMP**, marque el recuadro de selección **Comparación de host de subnodo** para comparar sucesos con subnodos. Si el grupo de atributos de sucesos de SNMP forma parte de un subnodo, puede marcar el recuadro de selección **Comparación de host de subnodo** para controlar si el sucesos debe proceder del agente SNMP que se supervisa.

   Por ejemplo: ha definido un agente para supervisar direccionadores, en el que cada instancia de subnodo representa un direccionador específico. Ha desarrollado un agente para recopilar datos de un direccionador con el recopilador de datos SNMP. También ha definido un grupo de atributos para recibir los sucesos de SNMP enviados por ese direccionador. Cada instancia de direccionador incluye los mismos datos definidos para el filtro de sucesos. Por lo tanto, necesita otra forma de asegurarse de que los sucesos del direccionador se muestran en el grupo de atributos de ese direccionador.

   Cuando la comparación de host de subnodo está seleccionada, un suceso que envía el direccionador se compara con el host definido para el recopilador de datos de SNMP. Si el host en uso por el recopilador de datos SNMP es el mismo host que envió el suceso recibido, dicha instancia de subnodo procesará el suceso de SNMP. En caso contrario, el suceso pasará a la siguiente instancia de subnodo. La comparación de dirección sólo se aplica a subnodos. Los grupos de atributos de sucesos de SNMP no realizan comparaciones de dirección en el agente básico. Para que funcione la comparación de dirección, la definición de subnodo debe contener al menos un grupo de atributos de SNMP. El host de SNMP que SNMP utiliza para dicha instancia de subnodo es el host que se utiliza para la comparación.

   Si el recuadro de selección **Comparación de host de subnodo** no está marcado, las instancias de subnodo no realizan esta comparación adicional. Debe permitir al usuario configurar un filtro de OID diferente para cada subnodo en este caso. De lo contrario, no será necesario incluir los grupos de atributos de sucesos de SNMP en la definición de subnodo.

6. En la ventana **Información de sucesos de SNMP**, seleccione los sistemas operativos.
7. Opcional: Puede pulsar **Probar** en la ventana **Información de sucesos de SNMP** para iniciar y probar el agente.

   Para obtener más información, consulte “Prueba de grupos de atributos de sucesos de SNMP” en la página 1276
8. Opcional:

   En la ventana **Información de sucesos de SNMP**, pulse **Avanzado** para seleccionar **Opciones de filtrado y resumen de sucesos**. Para obtener más información, consulte el apartado “Filtrado y resumen de sucesos” en la página 1446.

   a) Cuando termine de seleccionar **Opciones de filtrado y resumen de sucesos**, vuelva a la ventana **Información de sucesos de SNMP**. Si ha seleccionado previamente **Sucesos personalizados** en

la ventana **Información de sucesos de SNMP**, pulse **Siguiente**, para seleccionar atributos clave, o si no salte al siguiente paso.

b) En la página Seleccionar atributos clave, pulse en uno o varios atributos clave para el grupo de atributos, o pulse **Produce una sola fila de datos**.

9. Pulse **Siguiente**, o pulse **Finalizar** si utiliza el asistente para nuevo agente para guardar el agente y abrir Agent Editor.
10.

Qué hacer a continuación

Para obtener información sobre la adición de más atributos, consulte "Creación de atributos" en la página 1230.

Propiedades de configuración de sucesos de SNMP

Determinadas propiedades de configuración se crean automáticamente al añadir un grupo de atributos de sucesos de SNMP al agente

Después de añadir un origen de datos, la configuración se visualiza en la página **Información de configuración de tiempo de ejecución** de Agent Editor. Por ejemplo, Figura 32 en la página 1275 muestra las secciones de configuración y algunas propiedades de configuración que se crean automáticamente cuando un grupo de atributos de sucesos de SNMP se añade al agente.

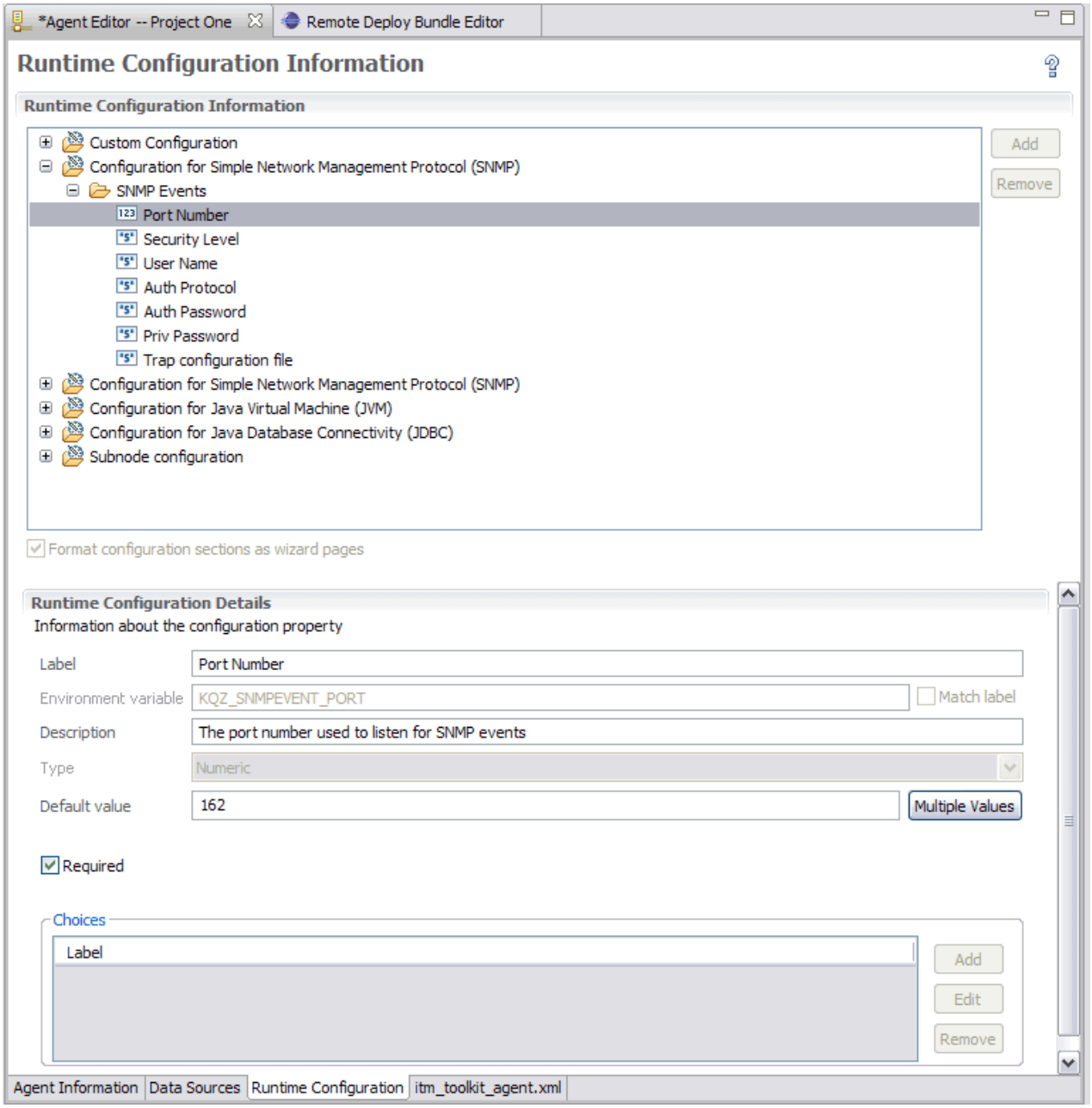


Figura 32. Página Configuración de tiempo de ejecución

Las etiquetas, descripciones y valores predeterminados de las propiedades de configuración predefinidas se pueden cambiar, pero los nombres y tipos de variable no se pueden cambiar. La sección Configuración de sucesos de SNMP contiene las siguientes propiedades:

Tabla 266. Propiedades de Configuración de sucesos de SNMP

Nombre	Valores válidos	Necesario	Descripción
Número de puerto	entero positivo	Sí	Número de puerto necesario que se utiliza para escuchar los sucesos
Nivel de seguridad	noAuthNoPriv, authNoPriv, authPriv	No	Nivel de seguridad de SNMP V3

Tabla 266. Propiedades de Configuración de sucesos de SNMP (continuación)			
Nombre	**Valores válidos**	**Necesario**	**Descripción**
Nombre de usuario	Serie	No	Nombre de usuario de SNMP V3
Protocolo aut.	MD5 o SHA	No	Protocolo de autenticación de SNMP V3
Contraseña aut.	Serie	No	Contraseña de autenticación de SNMP V3
Contraseña priv.	Serie	No	Contraseña de privacidad de SNMP V3
Archivo de configuración de condiciones de excepción	Nombre de archivo que incluye la vía de acceso	No	Ubicación del archivo de configuración de condiciones de excepción. Si el archivo no se localiza utilizando esta propiedad de configuración, se intenta encontrar un archivo `trapcnfg` en el directorio bin del agente.

No es necesaria ninguna configuración para sucesos V1 o V2C. Todos los sucesos V1 o V2C se procesan con independencia del origen o el nombre de comunidad especificados. El único protocolo de privacidad soportado es DES, así que no existe ninguna opción para especificar el protocolo de privacidad. Las opciones de configuración de SNMP V3 no son necesarias (cada una de ellas se puede especificar de manera opcional). Si desea especificarlas, debe especificar los valores adecuados para el nivel de seguridad que elija.

Prueba de grupos de atributos de sucesos de SNMP
Puede probar el grupo de atributos de sucesos de SNMP que ha creado, en Agent Builder.

Antes de empezar

Para probar el grupo de atributos de sucesos de SNMP, utilice un programa de prueba o aplicación para generar sucesos de SNMP.

Procedimiento

1. El procedimiento de prueba se puede iniciar de las siguientes formas:
   - Durante la creación del agente, pulse **Probar** en la página **Información sobre suceso de SNMP**.
   - Después de la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** de Agent Editor y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208

   Después de pulsar **Probar** en uno de los dos pasos anteriores, se abre la ventana **Probar valor de suceso**.
2. Opcional: Antes de empezar la prueba, puede establecer variables de entorno y propiedades de configuración. Para obtener más información, consulte "Prueba de grupo de atributos" en la página 1417. Para obtener más información sobre las propiedades de configuración de SNMP, consulte "Propiedades de configuración de sucesos de SNMP" en la página 1274.

3. Pulse **Iniciar agente**. Una ventana indica que el agente se está iniciando.

   Cuando el agente se inicia, escucha sucesos SNMP según su configuración.

   Nota: El agente que se inicia es una versión simplificada que incluye el grupo de atributos que está probando.
4. Para probar la recopilación de datos del agente, debe generar sucesos de SNMP que coinciden con la configuración de los agentes. Para ello, puede utilizar una aplicación o un generador de sucesos.

   Cuando el agente recibe sucesos de SNMP que coinciden con su configuración, añade los sucesos a su memoria caché interna.
5. Para simular una solicitud del entorno de supervisión para los datos de agente, pulse **Recopilar datos**.

   La ventana **Probar valores de sucesos** recopila y muestra los sucesos de la memoria caché del agente desde que se inició por última vez. Se muestra un ejemplo de recopilación de datos en la Figura 33 en la página 1277

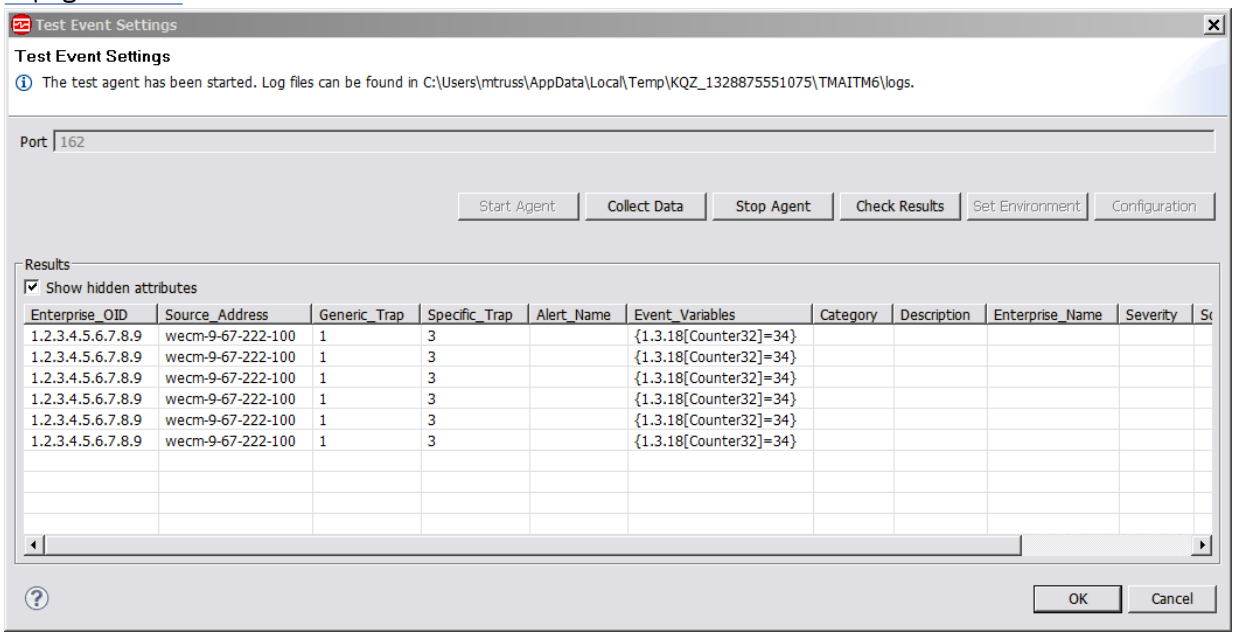


*Figura 33. Ventana **Probar valores de sucesos** que muestra los datos de sucesos de SNMP recopilados*

6. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Un ejemplo se muestra en la Figura 34 en la página 1277. Los datos que la ventana **Estado de la recopilación de datos** recopila y muestra se describen en "Nodo Estatus de objeto de rendimiento" en la página 1462

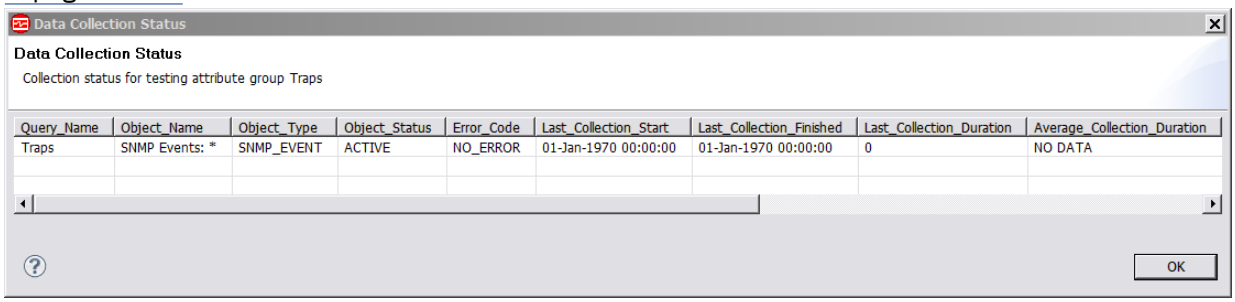


*Figura 34. Ventana **Estado de recopilación de datos***

7. Detenga el agente pulsando **Detener agente**.
8. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Probar valores de sucesos**. Al pulsar **Aceptar** se guardan los cambios que ha realizado.

Conceptos relacionados

"Pruebas del agente en Agent Builder" en la página 1417

Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión de MBeans Java Management Extensions (JMX)

Puede definir un origen de datos para recopilar datos de MBeans JMX. Los datos de todos los beans gestionados (MBeans) supervisados se colocan en un conjunto de datos. En función del MBean, el conjunto de datos puede producir una sola o varias filas.

Acerca de esta tarea

Cada origene de datos JMX que defina debe identificar un solo MBean (una sola instancia) o un determinado tipo de MBean (varias instancias). Debe conocer el Nombre de objeto del MBean o un patrón de Nombre de objeto para un tipo de MBean que contenga los datos que desea recopilar. Utilice un patrón de Nombre de objeto para identificar un conjunto de MBeans similares. El conjunto de MBeans que coincidan con el patrón deben proporcionar todos los datos que se deseen ver en la tabla de supervisión. Un patrón de Nombre de objeto típico será parecido al siguiente: `*:j2eeType=Servlet,*`. Este patrón de Nombre de objeto coincide con todos los MBeans que tienen un tipo de servlet j2eeType. Puede esperarse que cualquier MBean que coincida con este patrón tenga un conjunto similar de atributos expuestos y operaciones que se puedan añadir a su origen de datos. Un origen de datos que utilice este patrón recopilará datos de cada MBean que coincida con dicho patrón. Los atributos que defina para este origen de datos deben estar disponibles para cualquier MBean que coincida con el patrón de Nombre de objeto del origen de datos.

Se da soporte a Java versión 5 o posterior.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos de un servidor** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **JMX**.
3. Pulse **Siguiente**.
4. En la página **Información de JMX**, pulse **Examinar** para ver todos los MBeans JMX del servidor MBean.

   Después de definir el origen de datos, puede utilizar la función de examinar para llenar de modo previo la lista de atributos. Entonces, puede añadir atributos, eliminar atributos o modificar atributos de los que el navegador haya insertado. Los nombres de estos atributos pueden ser largos y difíciles de escribir correctamente. Utilizar la opción de búsqueda es una forma sencilla de introducir el nombre correcto.

   Nota: Puede crear manualmente orígenes de datos JMX especificando un Nombre de objeto y pulsando **Siguiente** sin utilizar el navegador. Cuando se crean manualmente orígenes de datos JMX se crean dos orígenes de datos. Se crea un origen de datos que contiene atributos para notificaciones JMX. Igualmente, se define un origen de datos que contiene un atributo que debe especificar en el asistente.

   Patrón de MBean
   Muestra el patrón de MBean.

   Opciones de JMX globales
   Muestra el nivel de soporte.

   Se proporciona soporte para los siguientes servidores JMX:

   - Servidor de MBean de sistema operativo Java 5. La conexión se realiza utilizando el conector JSR-160. Reciben soporte las notificaciones y los supervisores.
   - WebSphere Application Server, versión 6 y posteriores. Se proporcionan conectores para los protocolos SOAP y RMI. Los supervisores de JMX no están soportados porque un agente remoto no puede crear MBeans.

- WebSphere Community Edition y otros servidores de aplicaciones basados en Apache Geronimo. La conexión se realiza mediante conectores JSR-160 estándar. Las notificaciones y los supervisores de JMX reciben soporte en las versiones 1.1 y posteriores.
- JBoss Application Server, versión 4.0 y anteriores.
- JBoss Application Server, conexión JSR-160.
- WebLogic Server, versión 9 y posteriores. Se proporciona el conector para el protocolo T3.

5. La primera vez que se ejecuta el navegador de JMX, no hay elementos en el menú desplazable **Servidor MBean**. Para añadir conexiones, pulse el botón **Añadir**.

   Utilice el botón **Editar** para modificar o suprimir la conexión que ya ha definido y seleccionado en el menú desplegable. Las definiciones de conexión se almacenan en el espacio de trabajo de modo que, cuando cree una conexión, se recordará. Para crear una conexión, siga los pasos que se indican a continuación. Si ya dispone de una conexión, salte al paso siguiente.

   a) Para crear una conexión con un servidor MBeam, pulse **Añadir** para añadir una conexión o para editar una conexión existente.

      La ventana **Navegador JMX (Java Management Extensions)** se muestra cuando no hay conexiones definidas.

   b) Después de pulsar **Añadir** para añadir una conexión, se abre la página **Seleccionar tipo de conexión**.

   c) Utilice el Asistente de conexión del servidor MBean para conectarse a un servidor MBean. Las conexiones nuevas listadas en la página son selecciones que puede realizar para crear una conexión. Puede utilizar la lista de conexiones existente para crear una conexión nueva utilizando una conexión existente como plantilla. Seleccione uno de los tipos de conexión nueva y pulse **Siguiente** para empezar a crear una conexión.

   d) Después de seleccionar un tipo de conexión, es posible que se le solicite un tipo de conexión más específico. Se muestran dos plantillas basadas en el tipo de conexión **Conexiones JMX estándar (JSR-160)**. Seleccione la plantilla más apropiada para el servidor MBean y pulse **Siguiente**.

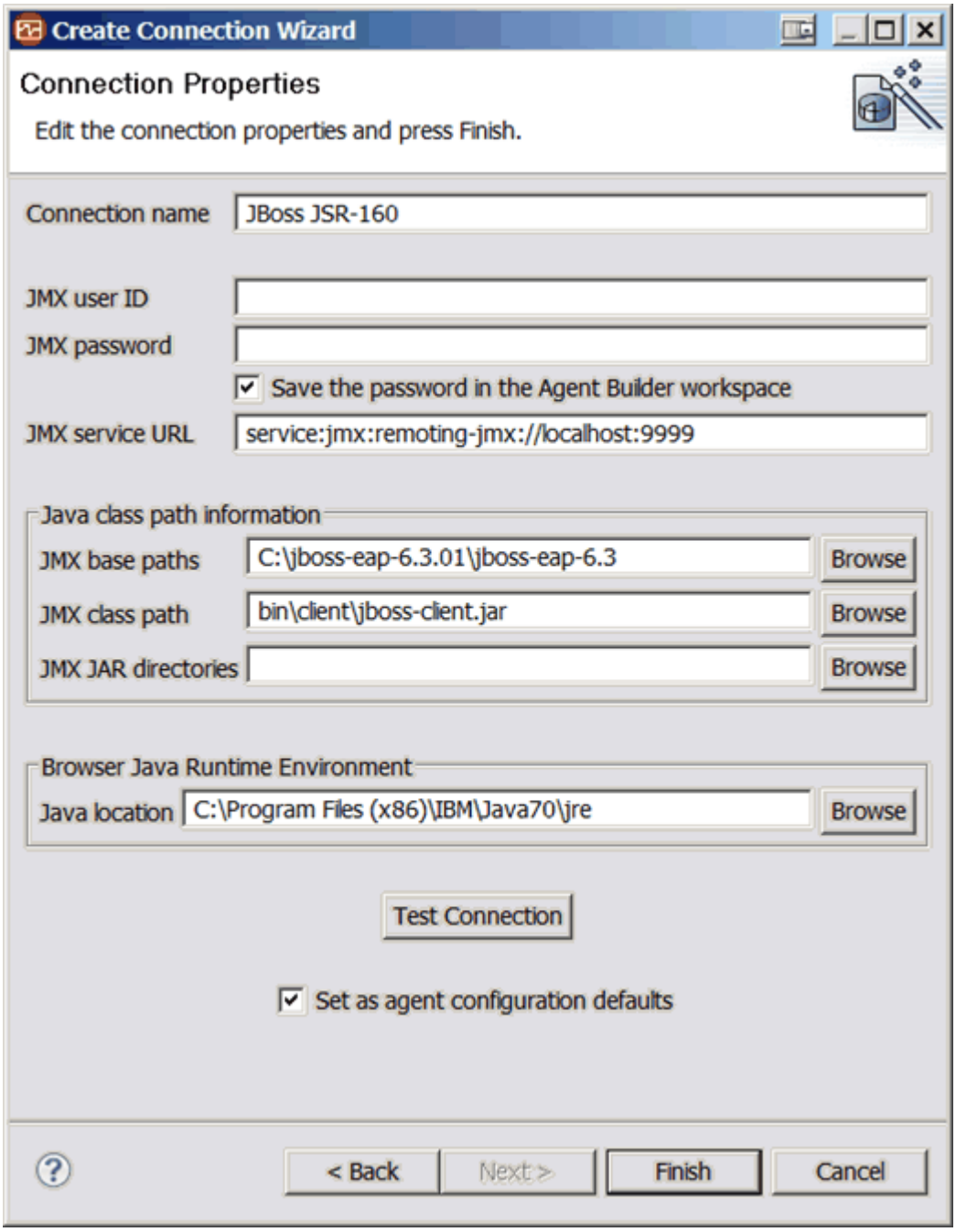


Figura 35. Propiedades de conexión JMX

La página **Propiedades de conexión** (Figura 35 en la página 1280) contiene los detalles de cómo conectarse a un servidor MBean. Debe completar la página con los detalles sobre el servidor MBean.

Importante: Si el origen de datos se conecta a un WebSphere Application Server remoto, asegúrese de que WebSphere Application Server también está instalado en el host que está ejecutando Agent Builder y establezca el valor de**Ubicación de Java** en el entorno de tiempo de ejecución Java que utiliza el WebSphere Application Server local.

e) Marque el recuadro de selección **Guardar la contraseña en el espacio de trabajo de Agent Builder** si desea guardar la contraseña para esta conexión.

f) Opcional: Seleccione **Establecer como valores predeterminados de configuración del agente** si desea que los valores predeterminados para JMX se copien de estas propiedades de conexión.

Por ejemplo, en Figura 35 en la página 1280 la **vía de acceso base JMX** predeterminada es `C:\jboss-eap-6.3.01\jboss-eap-6.3`, el **URL de servicio JMX** es `service:jmx:remoting-jmx://localhost:9999` y la **ubicación Java** es `C:\Archivos de programa\IBM\Java70\jre`

1) Después de especificar las propiedades necesarias para la conexión, pulse **Probar conexión** para asegurarse de que la conexión se puede establecer. Si la conexión no ha sido satisfactoria, corrija las propiedades necesarias.
2) Cuando la conexión sea satisfactoria, pulse **Finalizar** para volver al navegador que utiliza la conexión que ha configurado.

La información de la vía de acceso de clase Java en la página **Propiedades de conexión** contiene tres campos. Estos campos se deben completar según sea necesario para conectarse a un servidor MBean que requiera clases Java que no estén incluidas en el entorno en tiempo de ejecución de Java. Normalmente, el servidor MBean al que se desea conectar debe estar instalado en el mismo sistema que Agent Builder. En este caso, especifique el directorio en el que se instaló la aplicación que contiene el servidor MBean como el campo **Vías de acceso base de JMX**. El campo **Directorios JAR de JMX** listará los directorios en relación al directorio de Vías de acceso base que contiene los archivos JAR necesarios para conectarse al servidor MBean. El campo **Vía de acceso de clase JMX** se puede utilizar para incluir archivos JAR específicos. No es necesario que los archivos JAR que se enumeran en el campo **Directorios JAR de JMX** se listen por separado en el campo **Vía de acceso de clase JMX**.

Cualquiera de los campos puede contener más de una referencia; separe las entradas mediante un punto y coma. Estos valores son los mismos que se necesitan al configurar el agente. Para obtener más información, consulte (“Configuración de JMX” en la página 1285).

6. Después de seleccionar una conexión, el navegador de JMX descarga información sobre los MBeans del servidor JMX. Esta información se muestra en las cuatro áreas siguientes de la ventana **Navegador de JMX** (Figura 36 en la página 1282):

   Indicaciones para las pantallas que empiezan por la ventana Navegador de Java Management Extensions (JMX) Browser en el separador **Configuración de tiempo de ejecución** de Agent Editor: en la página **Información de JMX**, seleccione **Examinar**. En el navegador (Navegador de JMX sin ninguna conexión seleccionada), seleccione **Añadir**. En la página **Selección de conexión JMX** seleccione **JBoss** y, a continuación, **Siguiente**. En la página **Propiedades de conexión de JMX**, personalice dos Propiedades de conexión: Proveedor de JBoss URL: `jnp://wapwin3.tivlab.raleigh.ibm.com:1099/` y **Directorios Jar de JBoss**: la vía de acceso completa al directorio que contiene los siguientes archivos JAR: `jbossall-client.jar`, `jboss-jmx.jar`, `jboss-jsr77-client.jar`, `jboss-management.jar`. Seleccione **Finalizar**. Esta configuración define la conexión JBoss para que pueda obtener pantallas similares a las que se muestran aquí.

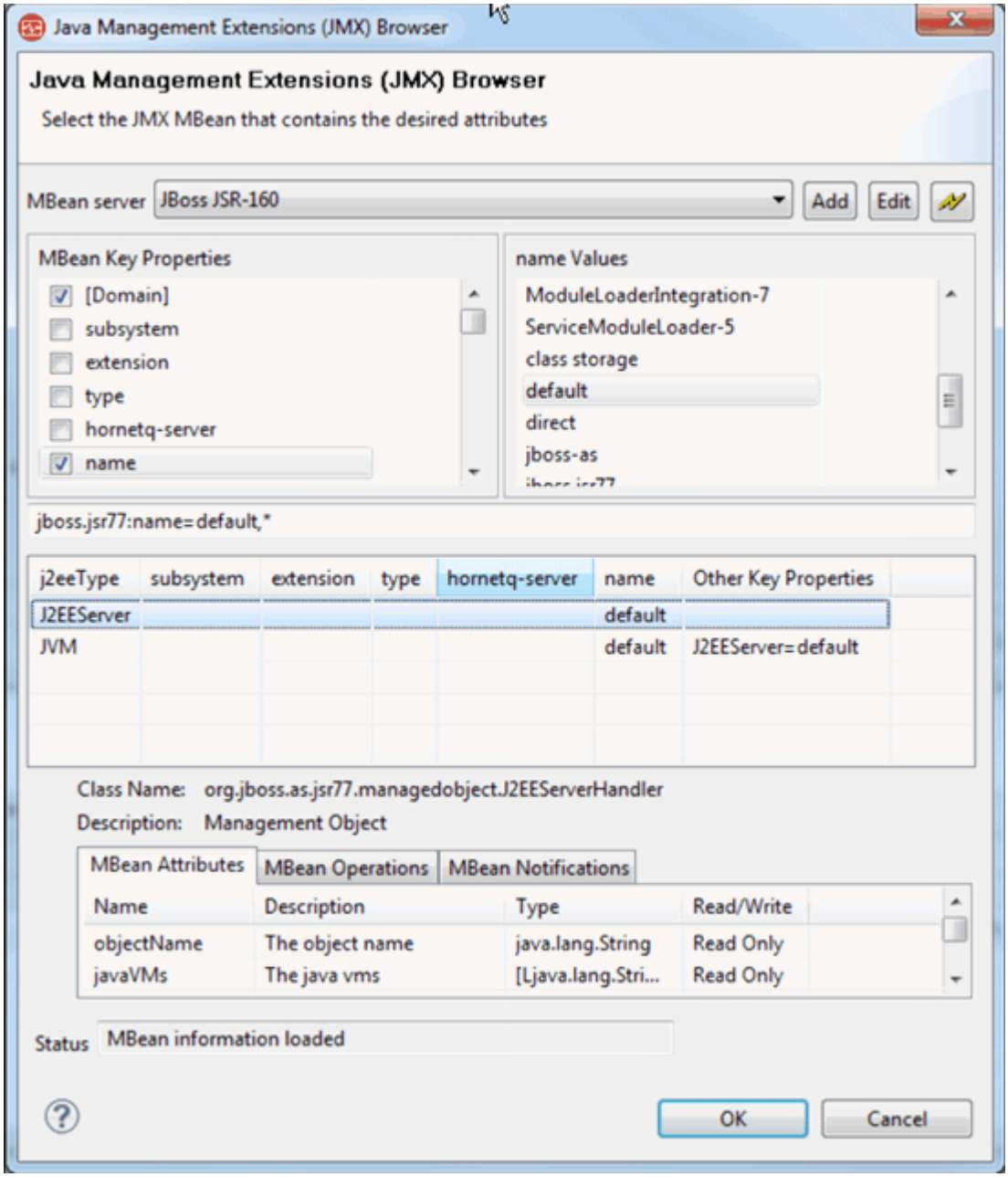


Figura 36. Ventana Navegador de Java Management Extensions (JMX)

- Área **Propiedades clave de MBean**: esta área es una recopilación de todas las claves exclusivas de Nombre de objeto encontradas en todos los MBeans en el servidor. La entrada **[Dominio]** es especial porque no es realmente una clave. Sin embargo, la entrada **[Dominio]** se trata como clave implícita para el valor del dominio del MBean. Seleccione un elemento de la lista y es encontrarán los MBeans que contienen esa propiedad de clave. La lista de valores de la propiedad clave se muestran en la lista **Valores de propiedades clave seleccionadas**. Cuando marque una propiedad de clave, se incluirá en el patrón de Nombre de objeto para el origen de datos.
- Área **Valores de propiedades clave seleccionadas**: esta área muestra los valores de la propiedad clave de MBean seleccionada actualmente de todos los MBeans. Al seleccionar uno de estos valores, se comprueba la propiedad de clave de MBean. La selección también actualiza el Patrón de nombre de objeto mostrado en el campo de mensaje con el nombre y el valor de la propiedad de clave de MBean.
- Una tabla lista todos los MBeans que coinciden con el Patrón de nombre de objeto: al seleccionar Propiedades de clave y valores en las listas Propiedades de clave de MBean y Valores de

propiedades de clave seleccionadas, se ve la actualización del Patrón de nombre de objeto. También se ve el cambio de la lista de MBeans en esta tabla para reflejar la lista de MBeans que coinciden con el patrón que ha seleccionado. Si tiene un patrón que no coincide con ningún MBean, puede borrar las entradas de la lista Propiedades de clave de MBean. Para borrar las entradas, pulse el recuadro de selección situado junto a una clave que el patrón utiliza y elimine la marca de selección. Además, puede editar manualmente los patrones para encontrar los MBeans que esté buscando. El patrón *:* selecciona todos los MBeans.

Puede utilizar esta tabla para examinar los MBeans del servidor y decidir cuáles contienen los datos que desea supervisar. Para facilitar la tarea de examinar un número de MBeans potencialmente elevado, puede ordenarlos por cualquier atributo de clave (en el menú o pulsando en una cabecera de columna). También puede mostrar cualquier atributo clave en cualquier columna seleccionando **Mostrar propiedad clave** en el menú. Cuando vea un valor de propiedad clave en la tabla que identifica los MBeans que desea supervisar, pulse con el botón derecho del ratón el valor y elija **Seleccionar solo MBeans con propiedad clave** en el menú.

- Una tabla que contiene detalles para un MBean seleccionado: el Navegador de JMX muestra información sobre un único MBean. Para ver los detalles de un MBean, debe seleccionar el MBean en la tabla que muestra una lista de MBeans que coinciden con el filtro actual. La información clave sobre el MBean es la lista de Atributos, Operaciones y Notificaciones que define.

Para crear un origen de datos desde el Navegador JMX, utilice los cuatro paneles descritos previamente para crear un Patrón de nombre de objeto. Cree el patrón de nombre de objeto para que coincida con un conjunto de MBeans que contengan, cada uno de ellos, los datos de supervisión que desee recopilar. Por ejemplo, si desea supervisar datos de todos los MBeans ThreadPool, utilice los siguientes pasos:

a) Seleccione **tipo** en el panel **Propiedades clave de MBean**. Si se selecciona **tipo** los valores de **Valores de propiedades clave seleccionadas** se actualizarán y listarán todos los valores exclusivos de la clave de tipo de cualquier MBean.

b) Seleccione **ThreadPool** en la lista de valores de clave de tipo. Después de seleccionar **ThreadPool**, el nombre de la propiedad clave de tipo se marcará en el panel **Propiedades clave de MBean** y el Patrón de nombre de objeto se actualizará a *:type=ThreadPool,*. La listase de MBeans también se actualiza para mostrar sólo los MBeans que coinciden con este patrón.

c) Seleccione uno de los MBeans en la lista de MBeans para ver los atributos, las operaciones y las notificaciones disponibles para el MBean. Si la lista de MBeans contiene más MBeans de los que desea supervisar, debe continuar este procedimiento de selección de propiedades y valores clave. Continúe hasta que tenga el Patrón de nombre de objeto que identifique el conjunto de MBeans que desea supervisar. También puede abrir un menú en la lista de MBeans para actualizar el Patrón de objeto con valores de propiedad clave mostrados en la tabla.

7. Cuando el patrón de nombre de objeto sea correcto, seleccione un MBean de la tabla.

   Todos los atributos del MBean seleccionado son los atributos iniciales en el nuevo origen de datos JMX. Es posible que algunos atributos no contengan datos. Después de crear el origen de datos JMX, revise los atributos y elimine cualquiera de ellos que no sea significativo. Si el MBean seleccionado no tiene atributos, se le avisa de que el origen de datos se va a crear sin atributos. Si el MBean seleccionado contiene notificaciones, también se crea un origen de datos de sucesos para recibir las notificaciones de los MBeans.

   Importante: Para cada atributo de MBean, Agent Builder crea un atributo en el conjunto de datos nuevo. Para un atributo de MBean numérico, Agent Builder crea un atributo numérico. Para cualquier tipo de objeto, incluido `String`, Agent Builder crea un atributo string que contiene una representación de serie del valor. Si un objeto de un atributo MBean es de tipo `javax.management.openmbean.CompositeData` y el explorador de Agent Builder puede leer el objeto, crea varios atributos, uno para cada objeto incorporado en el objeto `CompositeData`. Para incluir valores internos de un objeto que no sea un objeto `CompositeData` (campos o valores de retorno de método), debe crear un atributo que tenga un nombre de métrica más complejo, tal como se describe en “Campos específicos para MBeans Java Management Extensions (JMX)” en la página 1294.

8. Pulse **Finalizar** en la página Información de JMX.

Los orígenes de datos se crean en función del MBean seleccionado en el paso anterior. Si no se ha seleccionado ningún MBean, se crea un grupo de atributos sin atributos. Se muestra un aviso que le permite seleccionar un MBean. El origen de datos de notificación contiene la palabra **Event** (Suceso) al principio del nombre del origen de datos para distinguirlo del origen de datos que muestra atributos.

9. Para cambiar otras opciones de JMX para el agente, pulse **Opciones de globales**. Con estas opciones, puede:
   a) Elija si los supervisores de JMX están soportados por este agente. Si desea que se creen los grupos de atributos de supervisor y los mandatos de Actuación de JMX, seleccione **Incluir grupos de atributos y mandatos de actuación de JMX**

      Consulte el apartado siguiente para ver una descripción de los supervisores de JMX.

   b) Seleccione los tipos de servidores MBean a los que se conecta el agente cuando se despliega.

      Se listan varios tipos de servidores específicos de proveedor, junto con un servidor genérico compatible con JSR-160 para los servidores basados en estándares. Puede seleccionar tantos como necesite, pero debe seleccionar solo tipos de servidor que soporten los MBeans que se están supervisando. Debe seleccionar como mínimo uno. Si selecciona más de uno, se le solicitará que especifique en el momento de configurar el agente a qué tipo de servidor desea conectarse.
10. Pulse **Aceptar** después de seleccionar la opción que desee.
11. Opcional: Puede probar este grupo de atributos pulsando **Probar**. Para obtener más información sobre la prueba, consulte “Prueba de grupos de atributos de JMX” en la página 1296.
12. Opcional: Puede crear un filtro para limitar los datos devueltos por este grupo de atributos al pulsar **Avanzado**. Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte “Filtrado de grupo de atributos” en la página 1239
13. Pulse **Siguiente**.
14. En la página **Seleccionar atributos clave**, seleccione los atributos clave o indique que este origen de datos solo produce una fila de datos. Para obtener más información, consulte (“Selección de atributos clave” en la página 1208).
15. Pulse **Siguiente**.

    La ventana **Opciones para todo el agente JMX** muestra los tipos de servidores de aplicaciones a los que Agent Builder da soporte. Si seleccionó previamente **Establecer como valores predeterminados de configuración del agente** en la página **Propiedades de conexión**, el tipo de servidor de aplicaciones hasta el que navegó se selecciona automáticamente.
16. En la ventana **Opciones para todo el agente JMX** (Figura 37 en la página 1285), seleccione cualquier otro tipo de servidor de aplicaciones al que desee que el agente se pueda conectar.

    Nota: En el ejemplo que aparece, si elige **Conexión JBoss Application Server JSR-160** es igual que elegir **Servidor compatible con JSR-160** salvo que se suministran diferentes valores predeterminados.

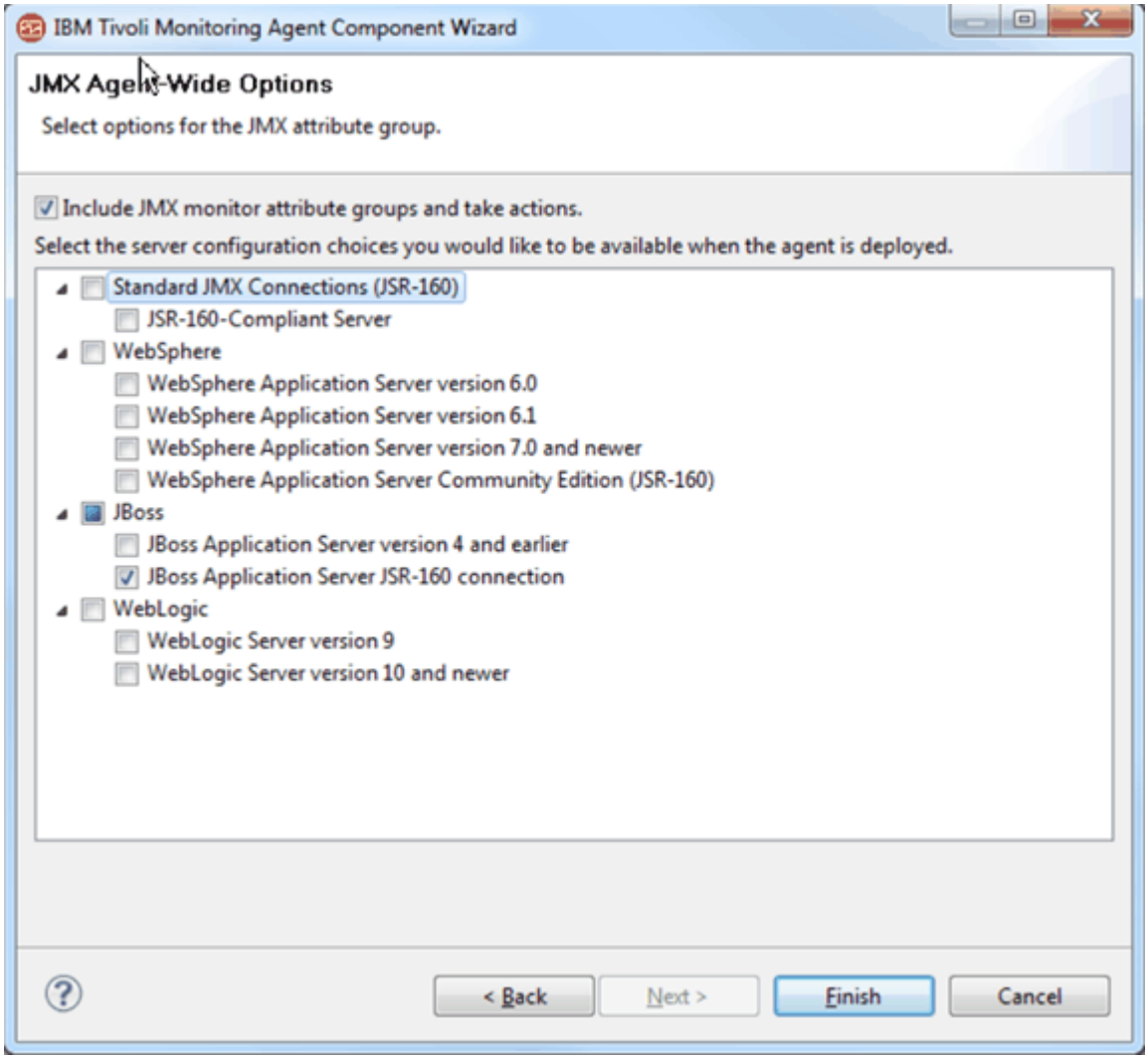


Figura 37. Ventana Opciones para todo el agente JMX

17. Realice una de las acciones siguientes:
    - Si utiliza el Asistente de agente nuevo, pulse **Siguiente**.
    - Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.
18. Si desea cambiar los tipos de servidores de aplicaciones a los que se puede conectar después de crear el agente, pulse **Opciones de JMX globales** en el área **Información de origen de datos JMX**.
19. En la ventana **Opciones para todo el agente JMX**, cambie todas las selecciones que desee.
20. Pulse **Aceptar**.
21. Para ver las secciones y las propiedades de configuración que se han generado automáticamente, pulse el separador **Configuración de tiempo de ejecución** de Agent Editor.

    El valor predeterminado de la propiedad `vías de acceso base JBoss` tiene el valor que se ha especificado en el navegador JMX.

Qué hacer a continuación

Si desea más información sobre los grupos de atributos para sucesos JMX, consulte "Grupos de atributos de Sucesos JMX" en la página 1490,

Configuración de JMX

Cuando se define un origen de datos JMX en el agente, parte de las propiedades de configuración se crean automáticamente.

La configuración de tiempo de ejecución de JMX es exclusiva debido a que proporciona cierto control sobre qué se muestra de la configuración. El cliente JMX para el agente puede conectarse a varios tipos diferentes de servidores de aplicaciones. Sin embargo, no es necesario dar soporte a todos estos tipos de servidores de aplicaciones en cualquier agente. Puede determinar qué tipos de servidores de aplicaciones se deben soportar, y las secciones de configuración innecesarias no se incluirán en el agente.

En la mayoría de los casos, un agente está diseñado para supervisar un tipo de servidor de aplicaciones JMX. Al crear el origen de datos JMX, puede utilizar el Navegador JMX. Cuando utiliza el Navegador JMX, las opciones de configuración del servidor JMX utilizadas para explorar el servidor MBean se añaden al agente automáticamente. Para cambiar los tipos de servidores de aplicaciones a los que puede conectarse después de crear el agente, pulse **Opciones de JMX globales** en el área **Información de JMX**. En la página **Opciones para todo el agente JMX**, cambie las selecciones que desee.

Puede diseñar un agente genérico que supervise más de un tipo de servidor de aplicaciones JMX. En este caso, se puede seleccionar más de una opción de configuración de servidor JMX en la página **Opciones para todo el agente JMX**. Cuando están soportadas más de un tipo de conexión JMX, la configuración de tiempo de ejecución le solicita el tipo de conexión que se utiliza para esa instancia de agente.

Nota: Una instancia de un agente sólo se puede conectar a un tipo de servidor de aplicaciones JMX. Se pueden utilizar subnodos para conectarse a diferentes servidores de aplicaciones JMX del mismo tipo dentro de una instancia de agente. Para conectarse a más de un tipo de servidor de aplicaciones JMX, debe configurar como mínimo una instancia de agente para cada tipo de servidor de aplicaciones JMX.

Puede ver, añadir y cambiar las propiedades de configuración utilizando Agent Editor. Encontrará instrucciones en: “Cambio de las propiedades de configuración utilizando Agent Editor” en la página 1404. Si un origen datos JMX está definido en un subnodo, también puede especificar Alteraciones temporales de configuración de subnodo. Encontrará instrucciones en: “Configuración del subnodo” en la página 1391.

Si define un origen de datos JMX en el agente, este debe utilizar Java para conectarse al servidor de aplicaciones JMX. Las propiedades de configuración de Java se añaden al agente automáticamente.

Las siguientes propiedades de configuración de Java son específicas de la configuración del tiempo de ejecución del agente:

Directorio inicial de Java
Vía de acceso completa que apunta al directorio de instalación Java

Configure el agente para que utilice la misma máquina virtual (JVM) que la que utiliza la aplicación que está supervisando, en concreto para WebLogic Server y WebSphere Application Server.

Argumentos de JVM
Especifica una lista opcional de argumentos para la máquina virtual Java.

Nivel de rastreo
Define la cantidad de información a escribir en el archivo de rastreo de Java. El valor predeterminado es grabar solo los datos de error en el archivo de registro.

Nota: El Agent Builder no requiere estas propiedades porque utiliza su propia JVM y registro, que se ha configurado a través del plug-in JLog.

Si se define un origen de datos JMX en el agente, los siguientes campos de configuración comunes necesarios se añaden al agente automáticamente:

Conexión
Tipo de conexión con el servidor MBean

ID de usuario
El ID de usuario que se utiliza para autenticarse en el servidor MBean.

Contraseña
Contraseña del ID de usuario.

Vías de acceso base
Directorios en los que se buscan archivos JAR nombrados en **Vía de acceso de clases** o directorios nombrados en **Directorios JAR**, que no estén calificados al completo. Los nombres de directorio están separados por un punto y coma (`;`) en Windows, y por un punto y coma (`;`) o dos puntos (`:`) en sistemas UNIX.

Vía de acceso de clases
Archivos JAR llamados explícitamente para que los busque el agente. Los que no están completamente calificados se añaden a cada una de las Vías de acceso hasta que se encuentra el archivo JAR.

Directorios de JAR
Directorios en los que se buscan archivos JAR. Los nombres de directorio están separados por un punto y coma (`;`) en Windows, y por un punto y coma (`;`) o dos puntos (`:`) en sistemas UNIX. No es necesario identificar explícitamente los archivos JAR de estos directorios; se encuentran porque residen en uno de estos directorios. No se busca en los subdirectorios de estos directorios. Cualquier nombre de directorio que no esté completamente calificado se añade a cada una de las Vías de acceso base hasta que se encuentra el directorio.

Nota: Para la supervisión remota, los archivos JAR y todos sus archivos JAR dependientes deben instalares localmente en el sistema donde se ejecuta el agente. Estos archivos JAR son archivos necesarios para conectarse a la aplicación que se está supervisando. Estos archivos JAR se deben configurar en **Directorios de JAR**, y en **Vías de acceso base** y **Vía de acceso de clase**. Además, instale localmente una JVM soportada para la aplicación que está supervisando y especifique la vía de acceso en el campo **configuración del Directorio inicial de Java**.

Ejemplos:

- Para WebLogic 10, la vía de acceso de clase es `server/lib/wlclient.jar;server/lib/wljmxclient.jar`. La vía de acceso base apunta al directorio del servidor de aplicaciones de WebLogic donde se encuentra el directorio `server/lib`.
- Para WebSphere, la vía de acceso base apunta a la ubicación donde está instalado el WebSphere Application Server. En este ejemplo se listan varias vías de acceso base para proporcionar un valor predeterminado para Windows y UNIX. La vía de acceso de clase lista los archivos JAR relativos a la vía de acceso base. El valor relativo `lib` para el campo **Directorios de JAR** hace que todos los archivos JAR de este directorio de la vía de acceso base se carguen.
  - **Vías de acceso base**: `C:\Archivos de programa\IBM\WebSphere\AppServer;/opt/IBM/WebSphere/AppServer`
  - **Vía de acceso de clase**: `runtimes/com.ibm.ws.admin.client_6.1.0.jar;plugins/com.ibm.ws.security.crypto_6.1.0.jar`
  - **Directorios de JAR**: `lib`

Según los tipos de servidor JMX que se seleccionan en la página Opciones para todo el agente JMX, se añaden todas o algunas de las propiedades de configuración siguientes. Los valores predeterminados los proporciona Agent Builder y se pueden modificar:

Propiedades compatibles con JSR-160 de configuración específicas de la conexión con el servidor:

URL del servicio JMX
URL de los servicios JMX al que se debe conectar para la supervisión.

Propiedades de configuración específicas de la conexión de WebSphere Application Server versión 6.0 y posteriores:

Nombre de host
Nombre de host del sistema donde se ubica el servidor de aplicaciones que está supervisando. Para la supervisión local, el nombre es el nombre del sistema local. Para la supervisión remota, el nombre es el nombre de host del sistema donde se ubica el servidor de aplicaciones.

Puerto
Número de puerto que utilizar en el nombre de host que se va a supervisar.

Protocolo de conectores
Protocolo de conectores que debe utilizar la conexión de supervisión. Se soportan RMI y SOAP.

Nombre de perfil
Nombre del perfil que se debe utilizar para configurar la conexión.

Propiedades de configuración específicas de la conexión con JBoss Application Server (no JSR-160):

Nombre JNDI
Nombre JNDI utilizado para realizar búsquedas en el servidor MBean.

URL de proveedor
URL del proveedor de servicios JMX al que se debe conectar para la supervisión.

Propiedades de la configuración específicas de la conexión de WebLogic Server:

URL de servicio
URL del proveedor de servicios JMX al que se debe conectar para la supervisión que incluye el nombre JNDI.

Nota: Si la seguridad administrativa de WebSphere está habilitada, debe asegurarse de que las solicitudes de inicio de sesión del cliente están inhabilitadas en los archivos de propiedades de conexión del cliente apropiados. Para conexiones RMI, para evitar que los clientes realicen solicitudes al usuario, debe modificar la propiedad *com.ibm.CORBA.loginSource* en el archivo `sas.client.props` en el directorio de propiedades de perfil del WebSphere Application Server. En una conexión SOAP, debe modificar la propiedad *com.ibm.SOAP.loginSource* en el archivo `soap.client.props` del mismo directorio. En ambos casos, la propiedad *loginSource* se debe establecer de modo que no contenga ningún valor.

Puede ver, añadir y cambiar las propiedades de configuración utilizando Agent Editor. Consulte (“Cambio de las propiedades de configuración utilizando Agent Editor” en la página 1404). Si un origen de datos de Windows se ha definido en un subnodo, también puede especificar Alteraciones temporales de configuración de subnodo. Consulte “Configuración del subnodo” en la página 1391.

Notificaciones de JMX
Además de proporcionar datos de supervisión cuando se solicitan, algunos MBeans también proporcionan notificaciones.

Una notificación es un objeto generado por un MBean que se pasa a los escuchas registrados cuando se produce un suceso.

Los agentes creados por Agent Builder pueden definir grupos de atributos que contengan valores de notificaciones en lugar de MBeans.

Cuando se inicia el agente, un `escucha de notificación` se registra con cada MBean que coincide con el patrón de MBean del grupo de atributos. Luego el grupo de atributos muestra una fila por cada notificación recibida. Cada columna contiene un elemento de datos de la notificación. Los datos deseados de la notificación se definen mediante un valor de columna de modo similar a como se definen los datos de columna para MBeans.

Para los grupos de atributos que no están basados en sucesos, los datos se recopilan cuando es necesario. Para los grupos de atributos basados en sucesos, el agente mantiene una memoria caché de los 100 últimos sucesos recibidos. Éstos se utilizan para responder a solicitudes de Tivoli Enterprise Portal. Los sucesos se reenvían inmediatamente para someterlos a análisis mediante situaciones y almacenamiento.

Supervisores de JMX
Además de proporcionar datos cuando se solicitan, algunos MBeans también proporcionan supervisores.

El proveedor JMX permite que un agente cree supervisores de JMX. Un supervisor de JMX es un MBean que el agente JMX crea en el servidor JMX. Supervisa el valor de un atributo de otro MBean y envía una notificación cuando el valor cumple algunos criterios. Se definen umbrales que permiten al supervisor informar sobre valores de atributos específicos.

No todos los servidores de aplicaciones soportan la creación de supervisores desde un cliente JMX, lo cual sí es cierto para los releases actuales de WebSphere Application Server. Los Supervisores de JMX y los mandatos de Actuación se pueden incluir en el agente seleccionado **Incluir grupos de atributos y actuaciones de supervisor de JMX** en **Opciones de JMX globales**.

Cualquier MBean que informe sobre un atributo de otro MBean se puede considerar un supervisor. En la práctica, JMX define tres clases de supervisor concretas, que son los tipos de supervisor que se crean. Están disponibles los tipos siguientes:

- Supervisor de cadenas – observa un atributo de cadena, informa sobre la igualdad o la no igualdad de esa cadena.
- Supervisor medidor – observa un atributo numérico variable e informa sobre movimientos ascendentes o descendentes que superen valores de umbral.
- Supervisor contador – observa un atributo numérico creciente e informa cuando alcanza un valor de umbral o aumenta en una determinada cifra.

Es posible que los grupos de atributos siguientes se añadan automáticamente al agente para recopilar o representar notificaciones de supervisores de JMX:

- `Supervisores registrados`

  Este grupo de atributos visualiza todos los supervisores de JMX que añade el usuario.
- `Notificaciones de contador`

  Este grupo de atributos informa de todas las notificaciones recibidas de Supervisores de contadores.
- `Notificaciones de medidores`

  Este grupo de atributos informa de todas las notificaciones recibidas de supervisores de medidores.
- `Notificaciones de cadena`

  Este grupo de atributos informa de todas las notificaciones recibidas de Supervisores de cadenas.

Mandatos de actuación para supervisores de JMX
Se crea un supervisor ejecutando un mandato de Actuación.

Se definen tres mandatos de Actuación, una para crear cada tipo de supervisor, y se define una cuarta actuación para suprimir un supervisor existente. Se aplica un límite de 256 caracteres a los mandatos de Actuación.

Los grupos de atributos de supervisión forman parte de cada agente JMX que se crea, incluidos todos los agentes creados por el Agent Builder. Los cuatro mandatos de Actuación están disponibles para todos los agentes, aunque no se pueden utilizar si no se trata de un agente JMX.

Observador de medida de adición de cadena de JMX
Utilice este mandato de actuación para crear un supervisor para observar un atributo de cadena.

Parámetros

Patrón de MBean
Este supervisor supervisa todos los MBeans que coinciden con este patrón.

Atributo observado
Nombre del atributo de cadena de MBean que se está observando.

Notificar coincidencia
El valor es true si se debe enviar una notificación cuando la cadena supervisada coincida con un valor de referencia, y false en caso contrario (el valor predeterminado es false).

Notificar diferencia
El valor es true si se debe enviar una notificación cuando la cadena supervisada no coincida con el valor de referencia, y false en caso contrario (el valor predeterminado es true).

Valor de referencia
Serie que se compara con el atributo observado.

Un valor predeterminado significa que el argumento no se ha especificado.

Ejemplo: Solicitar una notificación cuando un servicio se detenga

```
STRING_METRIC_WATCHER [*:type=Service,*] [StateString] [true] [false] [Stopped]
```

Donde:

`*:type=Service,*`
Patrón de MBean: supervisa cualquier MBean con un tipo con nombre de propiedad clave cuyo valor sea Service.

`StateString`
Atributo observado: un atributo de cadena que es común para todos los MBeans de `type=Service`.

verdadero
Notificar coincidencia: desea que se envíe una notificación a su agente cuando el atributo `StateString` coincida con el valor de referencia de Stopped.

falso
Notificar diferencia: no desea que se le notifique cuando el atributo Service no coincida con Stopped.

Detenido
Valor de referencia: cuando el atributo `StateString` cambia al valor Stopped, se envía una notificación.

Observador de medida de adición de medidor de JMX
Utilice este mandato de actuación para crear un supervisor que observe un atributo de indicador.

Parámetros

Patrón de MBean
Este supervisor supervisa todos los MBeans que coinciden con este patrón.

Atributo observado
Nombre del atributo de cadena de MBean que se está observando.

Modalidad de diferencia
El valor es true si el valor supervisado es la diferencia entre los valores actual real y anterior del atributo. El valor es false si el valor supervisado es el valor actual real del atributo (el valor predeterminado es false).

Notificar valor elevado
El valor es true si se debe enviar una notificación cuando un valor supervisado creciente supere el umbral superior, y false en caso contrario (el valor predeterminado es true).

Notificar valor bajo
El valor true si se debe enviar una notificación cuando un valor supervisado decreciente quede por debajo del umbral inferior, y false en caso contrario (el valor predeterminado es true).

Umbral superior
El valor por debajo del cual se espera que permanezca el atributo observado.

Umbral inferior
El valor por encima del cual se espera que permanezca el atributo observado.

Ejemplo: Solicitar una notificación cuando la memoria libre sea inferior a 10 Mb

```
GAUGE_METRIC_WATCHER [ServerInfo] [FreeMemory] [false] [false] [true] [30000000] [10000000]
```

Donde:

***:type=ServerInfo**
Patrón de MBean: supervisa cualquier MBean cuyo nombre tenga un tipo con nombre de propiedad de clave única cuyo valor sea ServerInfo.

FreeMemory
Atributo observado: un atributo numérico que fluctúa hacia arriba o hacia abajo, indicando la cantidad de memoria libre en el servidor de aplicaciones.

falso
Modalidad de diferencia: supervisa el valor de atributo real, no la diferencia entre una observación y otra.

falso
Notificar valor elevado: no se envía notificación cuando la memoria libre aumenta.

verdadero
Notificar valor bajo: no se envía notificación cuando la memoria libre disminuye demasiado.

30000000
Umbral superior: aunque no nos importa pasar un umbral superior, necesitamos un valor de umbral superior razonable. No se producirá una segunda notificación de umbral inferior hasta que el valor de atributo sea igual o mayor que el umbral superior.

10000000
Umbral inferior: es el valor de umbral inferior que deseamos que se nos notifique.

Observador de medida de adición de contador de JMX
Utilice este mandato de actuación para crear un supervisor que observe una atributo de contador.

Parámetros

Patrón de MBean
Este supervisor supervisa todos los MBeans que coinciden con este patrón.

Atributo observado
Nombre del atributo de cadena de MBean que se está observando.

Umbral inicial
Valor con el que se compara el atributo observado.

Desplazamiento
Valor añadido al umbral después de superar el umbral para crear un umbral cambiado.

Módulo
Valor máximo del contador después del cual se renueva a 0.

Modalidad de diferencia
El valor es true si el valor supervisado es la diferencia entre los valores actual real y anterior del atributo. El valor es false si el valor supervisado es el valor actual real del atributo (el valor predeterminado es false). Esta modalidad activa efectivamente la supervisión de velocidad de cambio.

Periodo de granularidad
Frecuencia con la que se realizan mediciones (el valor predeterminado es de 20 segundos). Es más importante si la modalidad de diferencia es true.

Ejemplo: Solicitar una notificación cuando cualquier servidor tenga tres errores o más.

```
COUNTER_METRIC_WATCHER [*:j2eeType=Servlet,*] [errorCount] [3] [4] [] [diff] [gran]
```

Donde:

`*:j2eeType=Servlet,*`
Patrón de MBean: supervisa cualquier MBean de servlet J2EE cuyo nombre tenga un tipo con nombre de propiedad clave única cuyo valor sea `ServerInfo`

`errorCount`
Atributo observado: atributo numérico creciente que indica el número de errores del servlet.

3
Umbral inicial: desea que se le notifique cuando `errorCount` sea igual o superior a 3.

4
Desplazamiento: cuando se recibe una notificación de tres errores, 4 es el umbral anterior de 3 para crear un nuevo umbral de 7. Se enviará una segunda notificación cuando `errorCount` llegue a 7; una tercera cuando llegue a 11; una cuarta a los 15, etcétera. Cero o ninguno no es válido porque se espera que el contador aumente siempre y no incrementar el desplazamiento no tendría ningún sentido para el contador.

Módulo:
errorCount no tiene un valor máximo definido, de modo que se debe utilizar un valor desmesuradamente elevado.

falso
Modalidad de diferencia: lo que nos importa son los recuentos de errores absolutos. El valor para la modalidad de diferencia sería true si nos interesara la tasa de aumento de errorCount.

Periodo de granularidad: no está establecido, de modo que se adoptará el periodo de granularidad predeterminado de 20 segundos. El periodo de granularidad está disponible para todos los tipos de supervisor. Sin embargo, se muestra con un supervisor de contador para que se pueda determinar una tasa de cambio significativa (con modalidad de diferencia=true).

Observador de medida de supresión de JMX
Utilice este mandato de Actuación para suprimir un supervisor.

Parámetro

Número
Número del supervisor tal como se muestra en la tabla REGISTERED_MONITORS.

Ejemplo: Suprimir el supervisor número 2

```
DELETE_WATCHER [2]
```

Donde:

2=
Número del supervisor que se va a suprimir.

Operaciones de JMX
Además de proporcionar datos de supervisión cuando se solicitan, algunos MBeans también proporcionan operaciones.

Los agentes que tienen orígenes de datos JMX incluyen el mandato de actuación `JMX_INVOKE` que se puede utilizar para ejecutar operaciones JMX en el servidor que se supervisa.

Sintaxis de los mandatos de Actuación

La acción tiene la siguiente sintaxis:

```
JMX_INVOKE [Patrón MBean] [Nombre operación] [Argumento 1] [Argumento 2]
[Argumento 3] [Argumento 4]
```

Donde:

Patrón de MBean
Consulta MBean que selecciona los MBeans en los que se ejecuta la operación. Si el patrón coincide con más de un MBean, la operación se ejecuta en cada uno de los MBeans coincidentes.

Nombre de operación
Nombre de la operación de MBean que se debe ejecutar.

Argumento 1, Argumento 2, Argumento 3, Argumento 4
Argumentos opcionales que se puede especificar para la operación de MBean. Los argumentos deben ser de un tipo de datos sencillo, como una serie o un entero.

El mandato de actuación `Invocar JMX` devuelve un resultado satisfactorio si la operación se ejecuta correctamente. Si la operación devuelve un valor, dicho valor se graba en el archivo de registro del proveedor de datos JMX.

Ejemplo: Iniciar una operación para restablecer un contador

Esta acción ejecuta la operación resetPeakThreadCount en los MBeans de tipo Threading:

```
JMX_INVOKE [*:type=Threading,*] [resetPeakThreadCount][] [] [] []
```

Donde:

:type=Threading,
Patrón de MBean: este patrón coincide con todos los MBeans que tienen el tipo Threading.

resetPeakThreadCount
Nombre de operación: la operación que se ejecuta en cada MBean que coincide con el patrón.

[] [] [] []
Argumento 1, 2, 3, 4: no se necesitan argumentos para esta operación. Solo se especifican para cumplir con la sintaxis de la acción.

Ejemplo: Iniciar una acción con un argumento

Esta acción ejecuta la operación getThreadCpuTime en los MBeans de tipo Threading. El resultado queda registrado en el archivo de rastreo del proveedor de datos JMX.

```
JMX_INVOKE [*:type=Threading,*] [getThreadCpuTime] [1] [] [] []
```

Donde:

:type=Threading,
Patrón de MBean: este patrón coincide con todos los MBeans que tienen el tipo Threading

getThreadCpuTime
Nombre de operación: la operación que se ejecuta en cada MBean que coincide con el patrón.

1
Argumento 1: el id de la hebra que se está consultando.

[] [] []
Argumento 2, 3, 4: estos argumentos no se necesitan para esta operación. Se especifican como argumentos vacíos para cumplir con la sintaxis del mandato de Actuación.

Ejecución del mandato de actuación JMX_INVOKE

El desarrollador del agente no puede esperar a que el usuario ejecute el mandato de actuación `JMX_INVOKE`. En su lugar, se deben desarrollar más acciones que ejecuten la Actuación `JMX_INVOKE`. Si es posible en estas acciones, oculte ante el usuario los detalles como el nombre de la operación y el patrón de MBean.

Inicio y detención de supervisores de JMX
Los supervisores de JMX son persistentes entre los inicios y detenciones del agente y el servidor JMX.

Si el agente detecta que el servidor JMX se ha reciclado, vuelve a registrar los supervisores. Si el agente se recicla, los supervisores se volverán a registrar. Las definiciones de los supervisores se almacenan en un archivo denominado `default_`*`nombreInstancia`*`.monitors` donde *nombreInstancia* es el nombre de la instancia del agente o el valor predeterminado si se trata de un agente de una sola instancia. Este archivo se encuentra en el siguiente directorio (tenga en cuenta que *xx* indica el código de producto de dos caracteres):

- Sistemas Windows: `TMAITM6/k`*`xx`*`/config`
- Sistemas UNIX y Linux: *`architecture`*`/`*`xx`*`/config` (consulte “Nuevos archivos en el sistema” en la página 1434 para obtener información sobre cómo determinar el valor de la arquitectura)

Si el agente se reinicia, utiliza el archivo de definiciones de supervisores para restaurar los supervisores.

Campos específicos para MBeans Java Management Extensions (JMX)
La sintaxis del nombre de medida para un grupo de atributos JMX debe seguir determinadas reglas cuando se especifican en la ventana **Información de atributo**.

La sintaxis del nombre de medida para un grupo de atributos JMX consta de señales separadas por un punto. Las señales forman valores primarios y, opcionalmente, valores secundarios:

- **Valor primario**: un valor obtenido directamente del MBean o de la Notificación en una fila específica de la tabla. Los valores primarios de un MBean se obtienen de un atributo de MBean o bien de la invocación de una operación de MBean (llamada a método). Los valores primarios de una Notificación se obtienen de un campo o invocación de un método sobre el objeto Notificación. Los valores primarios pueden ser tipos primitivos o pueden ser objetos Java.
- **Valor secundario**: un valor obtenido mediante el procesamiento posterior de un valor primario u otro valor secundario. Los valores secundarios se procesan internamente al motor y no implican llamadas al servidor JMX. Si el valor primario (u otro secundario) es un objeto Java, un valor secundario es el resultado de captar un campo público de ese objeto. Un valor secundario también puede ser el resultado de una llamada a método en ese objeto. Estos valores secundarios se obtienen utilizando la introspección Java del objeto Java primario (u otro secundario). Si el valor primario (u otro secundario) es una cadena Java en forma de nombre de MBean, el valor secundario puede ser el dominio. El valor secundario también puede ser cualquiera de las propiedades que componen el nombre de MBean.

La siguiente sintaxis describe el formato para el campo **Nombre de medida**:

```
Nombre de medida    =    valor_primario [ .valor_secundario ]
PrimaryValue    =    Attribute.nombre_atributo |
        Method.nombre_método |
        Domain |
        Property.nombre_propiedad |
        Field.nombre_campo |
        Nombre
Valor_secundario    =    Campo.nombre_campo |
        Method.nombre_método |
        Domain |
        Property.nombre_propiedad |
        Explode |
        ElementCount
```

```
propertyName    =    nombre de una propiedad clave en un nombre de objeto de MBean
attributeName    =    nombre de un atributo MBean
methodName    =    operación de argumento cero de un MBean o método de argumento cero
de una notificación u otro objeto Java.
nombreMétodo(argumento)    =    operación de un solo argumento de un MBean o un método
de un solo argumento de una Notificación u otro objeto Java. La
argumento se pasará al método como una serie.
fieldName    =    nombre de una variable de instancia pública en una notificación u
otro objeto de Java
notificationMethod    =    nombre de un método de argumento cero público de un
objeto de notificación
```

Al incluir sólo un valor primario en la definición del nombre de la medida, los datos recopilados pueden ser cualquiera de los siguientes elementos:

- Dominio de MBean
- Valor de serie de MBean
- Propiedad clave del nombre de MBean
- Valor de atributo numérico o de cadena en un atributo de MBean (incluido el nombre completo de otro MBean). Un valor de retorno numérico o de cadena de una operación de un MBean.
- Valor de una variable de instancia pública numérica o de cadena en un objeto Notificación
- Valor de retorno numérico o de cadena de una operación de una Notificación.

Mediante la adición de un valor secundario a la definición de una medida, puede detallar más el valor primario de un objeto Java. También puede iniciar un método público o captar una variable de instancia pública.

Mediante la adición de un valor secundario a otro valor secundario en la definición de la medida, puede detallar más un objeto de valor secundario. Puede continuar hasta la profundidad máxima en la que están anidados los objetos dentro de un MBean o una Notificación.

Las señales que constituyen los valores primarios y secundarios son palabras clave o nombres. En la mayoría de los casos, una señal de palabra clave va seguida de una señal de nombre. La tabla siguiente muestra algunos ejemplos:

Ejemplo de nombre de la medida	Tipo de grupo de atributos	Descripción de los datos devueltos
`Dominio`	MBean	La parte del dominio del MBean (la parte anterior a los dos puntos).
`Nombre`	MBean	La representación de cadena completa del MBean.
`Attribute.serverVendor`	MBean	Atributo de MBean serverVendor.
`Method.getHeapSize`	MBean	El valor devuelto por getHeapSize() en el MBean.
`Property.j2eeType`	MBean	El valor de j2eeType se extrae del nombre del MBean.
`Field.Message`	Suceso (Notificación)	El campo **Mensaje** en una notificación.

Las palabras clave `Atributo`, `Método` y `Campo` pueden devolver objetos Java que contienen otros datos. Puede ejecutar operaciones en esos objetos añadiendo definiciones de valores secundarios. Más ejemplos:

Ejemplo de nombre de la medida	Tipo de grupo de atributos	Descripción de los datos devueltos
Attribute.deployedObject.Method.getName	MBean	Toma el atributo deployedObject del MBean y obtiene el resultado del método getName().
Attribute.eventProvider.Method.getException.Method.getDescription	MBean	Va a tres niveles de profundidad: se supone que un atributo denominado eventProvider es un objeto que tiene un método getException(). Este método devuelve un objeto con un método getDescription(). Se llama a dicho método y el valor de retorno se coloca en la columna.
Attribute.HeapMemoryUsage.Method.get(used)	MBean	Toma el atributo HeapMemoryUsage del MBean y obtiene el resultado del método get(valor de cadena). La cadena utilizada se pasa al método como el argumento. Solo se puede proporcionar un argumento y debe ser un valor de cadena literal. Muestra cómo puede recopilar datos de una estructura de datos compuesta de un MBean abierto.

`Dominio` y `Propiedad` se pueden utilizar como palabras clave en valores secundarios si el valor anterior ha devuelto una cadena en formato de un nombre de MBean. Por ejemplo:

Ejemplo de nombre de la medida	Tipo de grupo de atributos	Descripción de los datos devueltos
`Attribute.jdbcDriver.Property.name`	MBean	El atributo jdbcDriver devuelve un nombre de MBean y la propiedad clave, name, se extrae del nombre del MBean.
`Attribute.jdbcDriver.Domain`	MBean	El atributo jdbcDriver devuelve un nombre de MBean y el dominio se extrae del nombre del MBean.

Las palabras clave `ElementCount` y `Explode` ejecutan operaciones en matrices o colecciones de datos.

- `ElementCount` – devuelve el número de elementos de una matriz.
- `Explode` – desglosa una fila en varias filas, una fila nueva para cada elemento de una matriz.

Ejemplos de las palabras clave:

Ejemplo de nombre de la medida	Tipo de grupo de atributos	Descripción de los datos devueltos
Attribute.deployedObjects.ElementCount	MBean	El atributo deployedObjects de MBean es una matriz, y esta columna contiene el número de elementos de la matriz.
Attribute.deployedObjects.Explode.MBean.Property.j2eeType	MBean	Hace que la tabla tenga una fila para cada elemento en los objetos desplegados. Esta columna contiene el j2eeType del objeto desplegado.
Attribute.SystemProperties.Method.values.Explode.Method.get(key)	MBean	Hace que el usuario obtenga una nueva fila por cada entrada de una estructura de datos tabular de MBean abierto. Cada estructura de datos tabular contiene una estructura de datos compuesta con un elemento llamado key, que se devuelve.

Prueba de grupos de atributos de JMX

Puede probar el grupo de atributos JMX que ha creado dentro de Agent Builder.

Procedimiento

1. El procedimiento de prueba se puede iniciar de las siguientes formas:
   - Durante la creación del agente, pulse **Probar** en la página **Información de JMX**.
   - Tras la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** del Agent Editor y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208.

   Tras pulsar **Probar** en uno de los dos pasos anteriores, se muestra la ventana **Prueba de JMX**.
2. Seleccione una conexión en la lista disponible en **Nombre de conexión** o bien pulse **Añadir** para añadir una conexión y siga el procedimiento detallado en "Supervisión de MBeans Java Management Extensions (JMX)" en la página 1278.
3. Opcional: Antes de iniciar la prueba, puede establecer variables de entorno, propiedades de configuración e información de Java.

   Para obtener más información, consulte "Prueba de grupo de atributos" en la página 1417. Para obtener más información sobre la configuración de JMX, consulte "Configuración de JMX" en la página 1285.
4. Pulse **Iniciar agente**.

   Una ventana indica que el agente se está iniciando.

5. Pulse **Recopilar datos** para simular una solicitud de datos de agente de Tivoli Enterprise Portal o de SOAP.

   El agente supervisa el servidor JMX en busca de datos. La ventana **Prueba de JMX** recopila y muestra los datos en la memoria caché del agente desde la última vez que se inició.
6. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana Estado de recopilación de datos recopila y muestra, se describen en "Nodo Estatus de objeto de rendimiento" en la página 1462
7. Detenga el agente pulsando **Detener agente**.
8. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Prueba de JMX**. Al pulsar **Aceptar** se guardan los cambios realizados.

Conceptos relacionados

"Pruebas del agente en Agent Builder" en la página 1417
Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión de datos procedentes de un CIM (Common Information Model)

Puede definir un origen de datos para que reciba datos de un origen de datos CIM (Common Information Model). Un origen de datos supervisa una sola clase CIM y coloca todos los valores de esta clase en el conjunto de datos que se genera. Si la clase proporciona varias instancias, el conjunto de datos tiene varias filas; puede filtrar por nombre de instancia para asegurarse de que el conjunto de datos tiene una fila.

Acerca de esta tarea

Esta tarea describe los pasos para configurar un origen de datos CIM (Common Information Model).

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos de un servidor** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **CIM**.
3. Pulse **Siguiente**.
4. En la página **Información de CIM (Common Information Model)**, en el área **Información de CIM**, realice una de las opciones siguientes:
   - Complete los campos **Espacio de nombres** y **Nombre de clase de CIM** para los datos que desea recopilar.
   - Pulse en **Examinar** para examinar un repositorio de CIM en un sistema específico.

     Se muestra la ventana **Navegador de clases CIM (Common Information Model)**. Este navegador se conecta a un servidor CIM y le proporciona información sobre las clases que existen en ese servidor.

     Para buscar un sistema remoto, seleccione un sistema en la lista **Nombre de host** (si se ha definido alguno). De forma alternativa, pulse **Añadir** para añadir el nombre de host del sistema en el que el servidor CIM está ubicado.

     La sintaxis para especificar el nombre de host es `http[s]://`*`nombre_host`*`:`*`puerto`*. Si solo proporciona el nombre de host, el navegador de clases de CIM (Common Information Model) se conecta utilizando el URL predeterminado `http://`*`hostname`*`:5988`.

     Si proporciona un protocolo sin especificar un puerto, se utiliza 5988 como valor predeterminado para `http` o 5989 como valor predeterminado para `https`.

     Si proporciona un puerto sin especificar un protocolo, se utiliza `http` con el puerto proporcionado.

Proporcione un ID de usuario y contraseña de una cuenta con permiso de lectura para los objetos del espacio de nombres que desea examinar. La ventana se actualiza con la información para el sistema remoto.

El Agent Builder intenta descubrir los espacios de nombres disponibles en el servidor CIM. Los espacios de nombres descubiertos se visualizan en la lista **Espacio de nombres**. No obstante, Agent Builder podría no descubrir todos los espacios de nombres disponibles en el servidor. Si desea examinar un espacio de nombres que no se encuentra en la lista **Espacio de nombres**, pulse el icono más (+) situado junto a la lista **Espacio de nombres**. Especifique el nombre del espacio de nombres en el campo y pulse **Aceptar**. Si el espacio de nombres está presente en el servidor CIM, se listarán las clases definidas en el espacio de nombres. Los espacios de nombres que escribe se guardan y colocan en la lista **Espacio de nombres** la próxima vez que examina ese servidor CIM en particular.

Cuando se selecciona un espacio de nombres en la lista **Espacio de nombres**, Agent Builder recopila toda la información de clase para ese espacio de nombres en particular. A continuación, Agent Builder coloca en memoria caché esta información para que se puede conmutar con rapidez entre espacios de nombres. Si desea forzar que Agent Builder recopile la información de clase para un espacio de nombres en particular, seleccione el espacio de nombres y pulse **Conectar**. Al pulsar **Conectar** se suprime la información almacenada en memoria caché y hace que Agent Builder recopile la información de clase.

Puede pulsar en el icono **Buscar** (binoculares) para buscar la selección en la lista. Escriba una frase en el campo **Frase de búsqueda**; especifique sus preferencias pulsando los campos **Buscar por nombre** o **Buscar por propiedades de clase** y pulse **Aceptar**. Si encuentra el elemento que está buscando, selecciónelo y pulse **Aceptar**.

5. En la página Información de CIM (Common Information Model), área **Sistemas operativos**, seleccione los sistemas operativos en los que debe tener lugar la recopilación.
6. Si ha escrito el espacio de nombres y el nombre de clase de CIM en el área **Información de CIM**, siga estos pasos:
   a) Pulse **Siguiente** para visualizar la página **Información de atributo** y definir el primer atributo en el grupo de atributos.
   b) Especifique la información sobre la página **Información de atributos** y pulse **Finalizar**.
7. Si ha examinado la información de CIM, se muestra la página Seleccionar atributos clave. En la página Seleccionar atributos clave, seleccione atributos clave o indique que este origen de datos solo genera una fila de datos. Para obtener más información, consulte (“Selección de atributos clave” en la página 1208).
8. Si ha navegado hasta la información de CIM, pulse en **Finalizar**.
9. Opcional: Puede probar este grupo de atributos pulsando **Probar**. Para obtener más información sobre la prueba, consulte “Prueba de grupos de atributos de CIM” en la página 1299
10. Opcional: Puede crear un filtro para limitar los datos devueltos por este grupo de atributos al pulsar **Avanzado**. Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte “Filtrado de grupo de atributos” en la página 1239
11. Realice una de las acciones siguientes:
    a) Si utiliza el **Asistente de agente**, pulse **Siguiente**.
    b) Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.

Configuración de CIM
Detalles sobre las propiedades de configuración de CIM.

Si define un origen de datos CIM en el agente, las propiedades de configuración de CIM se añaden al agente automáticamente. Puede ver, añadir y cambiar las propiedades de configuración utilizando Agent Editor. Si desea instrucciones, consulte “Cambio de las propiedades de configuración utilizando Agent Editor” en la página 1404). Si se define un origen de datos CIM en un subnodo, especifique Alteraciones temporales de configuración de subnodo. Encontrará instrucciones en: “Configuración del subnodo” en la página 1391.

Las siguientes propiedades de configuración específicas de la conexión se encuentran en la página de configuración de CIM:

CIM local o remoto
Autenticación local o remota para el servidor de CIM. El valor predeterminado de Local/Remota es Remota

ID de usuario de CIM
ID de usuario utilizado para acceder al servidor de CIM

Contraseña de CIM
Contraseña para acceder al servidor de CIM

Nombre de host CIM
Nombre de host al que se debe acceder para obtener datos de CIM

CIM sobre SSL
Utilice SSL para la comunicación con el servidor CIM. Las opciones son Sí y No. El valor predeterminado es No.

Número de puerto de CIM
Número de puerto utilizado para la comunicación que no es segura.

Número de puerto SSL de CIM
Número de puerto utilizado para la comunicación segura. El valor predeterminado es 5989. (El valor predeterminado para Solaris 8 normalmente es diferente).

Prueba de grupos de atributos de CIM
Puede probar el grupo de atributos CIM ha creado, dentro de Agent Builder.

Procedimiento

1. Inicie el procedimiento de prueba de las siguientes formas:
   - Durante la creación del agente, pulse **Probar** en la página **Información de CIM**.
   - Tras la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** del Agent Editor y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208

   Después de pulsar **Probar** en uno de los dos pasos anteriores, se visualiza la ventana **Probar valores**
2. Opcional: Establezca las variables de entorno y las propiedades de configuración antes de comenzar las pruebas.

   Para obtener más información, consulte "Prueba de grupo de atributos" en la página 1417.
3. Seleccione o añada un **Nombre de host**.

   Para obtener más información sobre la adición de un **Nombre de host**, consulte "Supervisión de datos procedentes de un CIM (Common Information Model)" en la página 1297
4. Pulse **Iniciar agente**.

   Se abre una ventana que indica que el agente se está iniciando.
5. Para simular una solicitud de Tivoli Enterprise Portal o SOAP para los datos de agente, pulse **Recopilar datos**.

   El agente consulta los datos en el servidor CIM. La ventana **Valores de prueba** recopila y muestra los datos en la memoria caché del agente desde que se inició por última vez.
6. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana **Estado de la recopilación de datos** recopila y muestra se describen en "Nodo Estatus de objeto de rendimiento" en la página 1462
7. Detenga el agente pulsando **Detener agente**.
8. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Probar valores**. Al pulsar **Aceptar** se guardan los cambios realizados.

Conceptos relacionados

"Pruebas del agente en Agent Builder" en la página 1417
Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión de un archivo de registro

Puede definir un origen de datos para recibir datos de un archivo de registro de texto. El agente analiza periódicamente las líneas que se añaden al archivo de registro y genera información del suceso basándose en estas líneas. Puede configurar el modo en que el agente analiza el registro en los sucesos. También puede configurar el agente para filtrar y resumir los datos. Los sucesos resultantes se colocan en un conjunto de datos.

Antes de empezar

Nota: El agente supervisa los archivos de registro que se encuentran en el mismo entorno local y página de códigos que en los que se ejecuta el agente.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos registrados** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **Un archivo de registro**.
3. Pulse **Siguiente**.
4. En la página **Información de archivo de registro**, escriba el nombre del archivo de registro que desea supervisar en el área **Información de archivo de registro**.

   El nombre del archivo debe estar calificado al completo.

   a) Opcional: Parte del nombre de archivo de registro viene de una propiedad de configuración de tiempo de ejecución. Para crear un nombre de archivo de registro, pulse **Insertar propiedad de configuración** y seleccione una propiedad de configuración.

   b) Opcional: El archivo también puede ser un nombre de archivo dinámico . Para obtener más información, consulte ("Soporte de nombres de archivo dinámicos" en la página 1540).
5. En el área **Identificación de campo**, pulse una de las opciones siguientes:

   Número fijo de caracteres
   Cuando se selecciona, limita el número de caracteres.

   Con esta opción, a cada atributo se le asigna el número máximo de caracteres que se puede retener de cada archivo de registro. Por ejemplo, si hay tres atributos A, B y C (en ese orden) y cada atributo es una cadena con una longitud máxima 20. Entonces, los 20 primeros bytes del registro van a A, los 20 siguientes van a B y los 20 siguientes a C.

   Separador de separadores
   Cuando se selecciona, permite utilizar separadores en los separadores.

   Separador de espacios
   Cuando se selecciona, se pueden utilizar varios espacios simultáneos como un único separador.

   Texto separador
   Cuando se selecciona, permite escribir el texto del separador.

   Texto inicial y final
   Cuando se selecciona, permite escribir el texto inicial y final.

   XML en elemento
   Si está seleccionado, escriba el nombre del elemento XML que desea utilizar como registro o pulse **Examinar** para definir el elemento.

   Si ha pulsado **Examinar**, se muestra la ventana **Navegador de XML**. Si utiliza la función de examinar, Agent Builder identifica todos los posibles atributos del registro examinando los códigos hijo y sus atributos.

Nota: A menos que pulse **Avanzado** y rellene la información de esta ventana, se supone lo siguiente acerca de la información que debe completar:

- Solo se supervisa un archivo de registro a la vez.
- Cada línea del archivo de registro contiene todos los campos necesarios para rellenar los atributos que deben definirse.

Para obtener más información sobre el análisis del archivo de registro y los separadores, consulte "Separadores y análisis de archivo de registro" en la página 1308.

6. Opcional: Pulse **Avanzado** en la página **Información de archivo de registro** para realizar lo siguiente utilizando la página **Propiedades avanzadas de origen de datos**:
   - Supervisar más de un archivo, supervisar archivos con nombres diferentes en distintos sistemas operativos o supervisar archivos con nombres que coinciden con expresiones regulares.
   - Trazar un conjunto de campos de más de una línea en el archivo de registro.
   - Elegir **Opciones de filtrado y resumen de sucesos**.
   - Producir información de resumen de salida. Este resumen produce un grupo de atributos adicional en cada intervalo. Para obtener más información sobre este grupo de atributos, consulte el apartado "Resumen de archivos de registro" en la página 1474. Esta función está en desuso por las opciones disponibles en el separador Información de suceso.

   a) Para supervisar más de un archivo de registro, pulse **Añadir** y escriba el nombre.

      Si se lista más de un archivo, debe especificarse una etiqueta exclusiva para cada archivo. La etiqueta puede mostrarse como atributo para indicar qué archivo ha generado el registro. No debe contener espacios.

   b) Opcional: Para seleccionar los sistemas operativos en los que se debe supervisar cada archivo de registro, siga estos pasos:

      1) Pulse en la columna **Sistemas operativos** para el archivo de registro.
      2) Pulse **Editar**.
      3) En la ventana **Sistemas operativos**, seleccione los sistemas operativos.
      4) Pulse **Aceptar** para guardar los cambios y volver a la página **Propiedades avanzadas de origen de datos**.

   c) Opcional: Seleccione **Los nombres de archivos coinciden con expresiones regulares** si el nombre de archivo que proporciona es una expresión regular que se utiliza para buscar el archivo en lugar de ser un nombre de archivo.

      Para obtener más información, consulte "Expresiones regulares de ICU" en la página 1530. Si no marca este recuadro, el nombre debe ser un nombre de archivo real. De forma alternativa, debe ser un patrón que siga las reglas para patrones de nombre de archivo que se describen en "Sintaxis de nombres de archivos dinámicos" en la página 1540.

   d) Opcional: Seleccione **Un elemento del directorio coincide con la expresión regular** para correlacionar un subdirectorio de la vía de acceso del nombre de archivo con una expresión regular.

      Puede seleccionar esta opción sólo si ha seleccionado también **Los nombres de archivo coinciden con la expresión regular** en el paso anterior.

      Si se utilizan metacaracteres de expresión regular en el nombre de vía de acceso, éstos se pueden utilizar en sólo un subdirectorio de la vía de acceso. Por ejemplo, puede especificar `/var/log/[0-9\.]*/mylog.*` para tener metacaracteres en un subdirectorio. `[0-9\.]*` correlaciona cualquier subdirectorio de `/var/log` que conste exclusivamente de números y puntos `(.)`. `mylog.*` correlaciona los nombres de archivo de estos subdirectorios `/var/log` que empiezan por `mylog` seguidos por cero o más caracteres.

      Dado que algunos sistemas operativos utilizan la barra inclinada invertida `(\)` como separador de directorios, ésta no se puede confundir con un metacarácter de escape de expresión regular. A causa de esta confusión, para indicar directorios se deben utilizar siempre barras inclinadas no invertidas. Por ejemplo, los archivos Windows especificados como `C:\temp\mylog.*` puede

significar que `\t` es un carácter de tabulador abreviado. Por lo tanto, utilice siempre barras inclinadas (`/`) en todos los sistemas operativos como separadores de directorios. El ejemplo `C:/temp/mylog.*` representa todos los archivos del directorio `C:/temp` que empiezan por `mylog`.

e) En la lista **Cuando coinciden varios archivos**, seleccione una de las opciones siguientes:

- **El archivo con el valor numérico más alto en el nombre de archivo**
- **El archivo de mayor tamaño**
- **El último archivo que se ha actualizado**
- **El último archivo que se ha creado**
- **Todos los archivos que coinciden**

Nota: Cuando se selecciona **Todos los archivos que coinciden**, el agente identifica todos los archivos del directorio que coinciden con el patrón de nombre de archivo dinámico. El agente supervisa las actualizaciones de todos los archivos en paralelo. Los datos de todos los archivos se entremezclan durante el proceso de recopilación de datos. Es mejor añadir un atributo seleccionando **Nombre de archivo de registro** en **Información de campos de registro** para correlacionar los mensajes de registro con los archivos de registro que contienen los mensajes de registro. Asegúrese de que todos los archivos que coinciden con el patrón de nombre de archivo dinámico se pueden dividir en atributos de manera coherente. Si los archivos de registro seleccionados no se pueden analizar de manera coherente, es mejor seleccionar **Todo el registro** en **Información de campos de registro** para definir un único atributo. Para obtener más información sobre la especificación de **Información de campos de registro** para atributos, consulte el paso "8" en la página 1304.

f) Seleccione la forma en que debe procesarse el archivo.

Con **Procesar todos los registros cuando se muestrea el archivo**, puede procesar todos los registros en todo el archivo cada vez que caduca el intervalo de muestreo definido para el supervisor de registro. El intervalo predeterminado es de 60 segundos. Este intervalo se puede modificar utilizando la variable de entorno *KUMP_DP_COPY_MODE_SAMPLE_INTERVAL* (especificando un valor en segundos). Cada vez se informa sobre los mismos registros a menos que éstos se eliminen del archivo. Con esta selección, no se generan datos de los sucesos cuando se graban registros nuevos en el archivo. Con **Procesar nuevos registros añadidos al archivo**, puede procesar los nuevos registros que se añaden al archivo mientras el agente está en ejecución. Se genera un registro de sucesos para cada registro añadido al archivo. Si el archivo se sustituye (el primer registro cambia de alguna forma), se procesa el archivo y se produce un suceso para cada registro del archivo.

Nota: Si se añaden registros a un archivo de registro XML, los registros añadidos deben contener un conjunto completo de elementos definidos en el elemento XML que ha seleccionado como **Identificación de campo**.

g) Si ha elegido procesar los nuevos registros que se añaden al archivo, también puede elegir cómo se detectan los nuevos registros.

Con **Detectar nuevos registros cuando aumenta el recuento de registros**, se pueden detectar los nuevos registros cuando el número de registros del archivo aumenta, si el tamaño del archivo cambia. Esta característica es útil cuando se asigna previamente todo un archivo de registro antes de grabar registros en el archivo. Esta opción se puede seleccionar para los archivos que no están asignados previamente, pero resulta menos eficaz que la supervisión del tamaño del archivo. Con **Detectar nuevos registros cuando aumenta el tamaño del archivo**, puede determinar cuándo se añade una nueva entrada a un archivo de la forma habitual. Puede que se produzca un pequeño retardo hasta que se reconozca que un archivo supervisado se ha sustituido.

h) Si ha seleccionado **Detectar nuevos registros cuando aumenta el tamaño de archivo**, también puede elegir cómo procesar un archivo que existe cuando se inicia el agente de supervisión.

Ignorar los registros existentes inhabilita la generación de sucesos para los registros que se encuentren en el archivo en el momento en que se inicie el agente. **Procesar ___ registros existentes del archivo** especifica la generación de un suceso para un número fijo de registros desde el final del archivo hasta el momento en que se inicia el agente. **Procesar registros no procesados previamente por el agente**: especifica que el agente de supervisión mantenga los

datos de reinicio para que el agente conozca los registros que se han procesado la última vez que se ha ejecutado. Se producen sucesos para todos los registros que se añaden al archivo desde la última vez que se ha ejecutado el agente. Esta opción implica un poco más de proceso cada vez que se añade un registro al archivo.

i) Si ha seleccionado **Procesar registros no procesados previamente por el agente**, puede elegir lo que se debe hacer cuando se inicia el agente y aparentemente se ha sustituido el archivo existente.

Procesar todos los registros si el archivo se ha sustituido: si la información sobre el archivo supervisado y la información de datos de reinicio no coinciden, se generan sucesos pata todos los registros en el archivo. Entre los ejemplos de no coincidencias se incluyen: el nombre de archivo es diferente, la hora de creación del archivo es diferente, el tamaño de archivo ha disminuido, la hora de la última modificación del archivo es anterior de la de antes. **No procese los registros si el archivo se ha sustituido**: si la información sobre el archivo supervisado y la información de datos de reinicio no coinciden, inhabilita el procesamiento de los registros existentes en el archivo.

j) Pulse la pestaña **Identificación de registro** para interpretar varias líneas en el archivo de registro como un solo registro lógico.

Nota: Si selecciona **XML en elemento** como la identificación del campo en la página **Información de archivo de registro**, el separador **Identificación de registro** no se visualiza.

- **Una sola línea** interpreta cada línea como un único registro lógico.
- **Línea de separador** una secuencia de caracteres que identifique una línea que separa un registro de otro.

  Nota: LA línea de separador no forma parte del registro anterior o siguiente.
- **Regla** identifica un número máximo de líneas que componen un registro y, opcionalmente, una secuencia de caracteres que indican el principio o el final de un registro. Con **Regla**, puede especificar las siguientes propiedades:
  - **Número máximo de líneas no en blanco** define el número máximo de líneas que no están en blanco que una regla puede procesar.
  - **Tipo de regla**: puede ser uno de los siguientes:
    - **Sin comparación de texto** (el número máximo de líneas por registro indica un único registro lógico).
    - **Identificar el principio de registro** (marca el inicio del único registro lógico).
    - **Identificar el final del registro** (marca el final del único registro lógico).
  - **Desplazamiento**: especifica la ubicación dentro de una línea en la que debe aparecer la cadena de comparación.
  - **Prueba de comparación**: puede ser **Es igual**, que requiere la coincidencia de una secuencia de caracteres en el desplazamiento específico, o **No es igual**, que indica que una secuencia de caracteres en particular no aparece en el desplazamiento específico.
  - **Cadena de comparación** define la secuencia de caracteres que comparar.
- **Expresión regular** identifica un patrón que se utiliza para indicar el principio o el final de un registro. Mediante la utilización de una **Expresión regular**, puede especificar las propiedades siguientes:
  - **Cadena de comparación** define la secuencia de caracteres con la que debe coincidir.

    O
  - Inicio o final de registro:
    - **Identificar el inicio de registro** marca el inicio del registro lógico único.
    - **Identificar el final de registro** marca el final del registro lógico único.

k) Si antes ha seleccionado **Procesar todos los registros cuando se muestrea el archivo**, pulse el separador **Expresión de filtro**. Al pulsar **Expresión de filtro** puede filtrar los datos que se

devuelven como filas en función de los valores de uno o varios atributos, variables de configuración, o de ambos.

Si antes ha seleccionado **Procesar nuevos registros añadidos al archivo**, no puede crear una expresión de filtro. Para obtener más información sobre el filtrado de datos de un grupo de atributos, consulte "Filtrado de grupo de atributos" en la página 1239.

l) Si anteriormente ha seleccionado **Procesar nuevos registros añadidos al archivo**, pulse la pestaña **Información de suceso** para seleccionar **Opciones de filtro y resumen de suceso**.

Para obtener más información, consulte ("Filtrado y resumen de sucesos" en la página 1446).

Nota: El separador Resumen puede estar presente si el agente se ha creado con una versión anterior de Agent Builder. El separador de resumen ha quedado obsoleto por el separador Información de suceso

7. Opcional: Pulse **Probar valores de archivo de registro** en la página **Información de archivo de registro** para iniciar y probar el origen de datos. . Pulse **Probar valores de archivo de registro** después de seleccionar las opciones para el origen de registro. Cuando prueba el origen de datos del archivo de registro y proporciona contenido de archivo de registro, Agent Builder crea los atributos en el grupo automáticamente, en función del resultado del análisis del registro. Para obtener más información sobre la prueba, consulte "Prueba de grupos de atributos de archivo de registro" en la página 1310.
8. Utilice los pasos siguientes si no ha utilizado la función de prueba previamente y ha escrito el nombre de archivo de registro en el área **Información de archivo de registro** de la página **Información de archivo de registro**:
   a) Pulse **Siguiente** para visualizar la página **Información de atributo** y definir el primer atributo en el grupo de atributos.
   b) Especifique la información en la página **Información de atributo** y pulse **Finalizar**.

   Nota: Cuando se añade un grupo de atributos de archivo de registro a un agente de la versión mínima predeterminada Tivoli Monitoring versión (6.2.1) o posterior, se incluye n grupo de atributos `Estado de archivo de registro`. Para obtener más información sobre el grupo de atributos `Estado de archivo de registro`, consulte "Grupo de atributos Estado del archivo de registro" en la página 1505.

   Junto con los campos aplicables a todos los orígenes de datos, la página **Información de atributo** para el origen de datos de archivo de registro tiene algunos campos adicionales en el área **Información de campo de registro**.

   Los campos **Información de campo de registro** son:

   Campo siguiente
   Muestra el siguiente campo después del análisis, utilizando los delimitadores del grupo de atributos (o delimitadores especiales para este atributo del diálogo Avanzado).

   Resto del registro
   Muestra el resto del registro después de que se analicen los atributos anteriores. Este atributo es el último, excepto posiblemente por el nombre de archivo de registro o la etiqueta de archivo de registro.

   Todo el registro
   Muestra el registro entero, que puede ser el único atributo, excepto para posiblemente el nombre o la etiqueta del archivo de registro.

   Nombre de archivo de registro
   Muestra el nombre del archivo de registro.

   Etiqueta de archivo de registro
   Muestra la etiqueta que se asigna al archivo en el panel avanzado.

   Nota: Utilice el separador **Detalles de atributo derivado** únicamente si desea un atributo derivado, no un atributo procedente directamente del archivo de registro.
9. Pulse **Avanzado** en el área **Información de campo de registro** para mostrar la página **Información avanzada de atributo de archivo de registro**.

a) En la sección **Filtros de atributos**, especifique los criterios correspondientes a los datos que se deben incluir o excluir.

   El filtrado de atributos puede mejorar el rendimiento de la solución al reducir la cantidad de datos que se procesan. Pulse uno o varios filtros de atributos:

   - **Inclusivo** indica que el conjunto de filtros de atributos es un filtro de aceptación, lo que significa que si el filtro es satisfactorio, el registro pasa el filtro y aparece en la salida.
   - **Exclusivo** indica que el conjunto de filtros de atributos es un filtro de rechazo, lo que significa que si el filtro de atributos es satisfactorio, el registro se rechaza y no aparece en la salida.
   - **Coincidencia con todos los filtros** indica que todos los filtros definidos en el filtro deben coincidir con el registro de atributos para que el filtro sea satisfactorio.
   - **Coincidencia con algún filtro** indica que si cualquiera de los filtros definidos en el filtro coincide el registro de atributos, el filtro es satisfactorio.

b) Utilice **Añadir**, **Editar** y **Eliminar** para definir los filtros individuales para el conjunto de filtros de atributos.

c) Para añadir un filtro, siga estos pasos:

   1) Pulse **Añadir** y complete las opciones de la ventana **Añadir filtro** del modo siguiente:

      a) La sección **Criterios de filtro** define las características básicas del filtro, incluidas las siguientes propiedades:

         - **Desplazamiento inicial** define la posición en la cadena de atributo en la que debe comenzar la comparación.
         - **Cadena de comparación** define la cadena de patrón sobre la que se define el atributo.

           Escriba una cadena, un patrón o una expresión regular que el agente utilizará para filtrar los datos que se lean del archivo. Los registros que coinciden con el patrón del filtro se eliminan de los registros que se han devuelto al entorno de supervisión, o son los únicos registros devueltos. El resultado depende de si elige que el filtro sea inclusivo o exclusivo.
         - **Coincidir todo el valor** comprueba si hay una aparición exacta de la cadena de comparación en la cadena de atributo. La comprobación empieza a partir de la posición de desplazamiento de inicio.
         - **Coincidir cualquier parte de valor** comprueba la cadena de comparación en cualquier lugar de la cadena de atributo. La comprobación empieza a partir de la posición de desplazamiento de inicio.

      b) **La cadena de comparación es una expresión regular** indica que la cadena de comparación es un patrón de expresión regular que se puede aplicar en la cadena de atributo.

         Se proporciona soporte de filtrado de expresiones regulares utilizando las bibliotecas ICU (International Components for Unicode) para comprobar si el valor de atributo examinado coincide con el patrón especificado.

         Para utilizar eficazmente el soporte de expresiones regulares, debe estar familiarizado con los detalles de cómo ICU implementa expresiones regulares. Esta implementación no es idéntica a cómo el soporte de expresiones regulares se implementa en expresiones regulares `Perl`, `grep`, `sed`, Java y otras implementaciones. Consulte "Expresiones regulares de ICU" en la página 1530 para obtener instrucciones sobre cómo crear filtros de expresiones regulares.

      c) **Definir un filtro de alteración temporal** indica que desea proporcionar una comparación de filtro más específica que altere temporalmente las características básicas previamente definidas. Esta cadena de comparación adicional se utiliza para invertir el resultado de filtro. Cuando el filtro es **Inclusivo**, la alteración temporal actúa como calificador de exclusión para la expresión de filtro. Cuando el filtro es **Exclusivo**, la alteración temporal actúa como calificador de inclusión para la expresión de filtro. (Si desea más información sobre **Inclusivo** y **Exclusivo**, consulte el paso "9" en la página 1304, y los ejemplos que le siguen). El filtro de alteración temporal tiene las siguientes propiedades:

- **Desplazamiento inicial** define la posición en la cadena de atributo en la que debe comenzar la comparación.
- **Cadena de comparación** define la cadena de patrón con la que se hace coincidir el atributo.

  Escriba una expresión regular que el agente utilizará para filtrar los datos que se leen del archivo. Los registros que coinciden con el patrón del filtro se eliminan de los registros que se han devuelto al entorno de supervisión, o son los únicos registros devueltos. El resultado depende de si elige que el filtro sea inclusivo o exclusivo.

d) **Valor de sustitución** se puede utilizar para modificar la cadena de atributo con un nuevo valor. Consulte "Expresiones regulares de ICU" en la página 1530 para ver más detalles sobre los caracteres especiales que se pueden utilizar.

e) **Sustituir primera aparición** sustituye la primera aparición que coincide con la cadena de comparación por texto nuevo.

f) **Sustituir todas las apariciones** sustituye todas las apariciones que coinciden con la cadena de comparación por texto nuevo.

2) Pulse **Aceptar**.

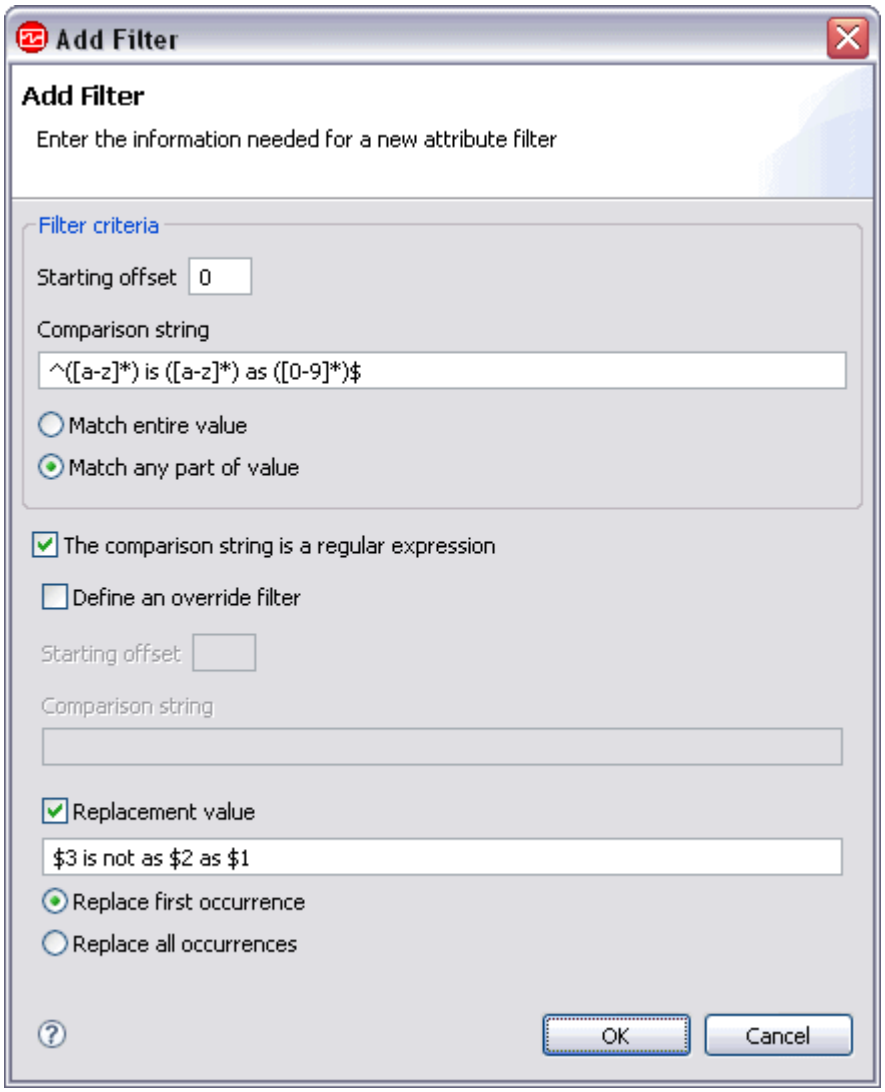


*Figura 38. Ejemplo 1 de **Añadir filtro***

Si la cadena de atributo es `abc is easy as 123`, se muestra la cadena sustituida en el Tivoli Enterprise Portal o la consola IBM Cloud Application Performance Management como `123 is not as easy as abc`.

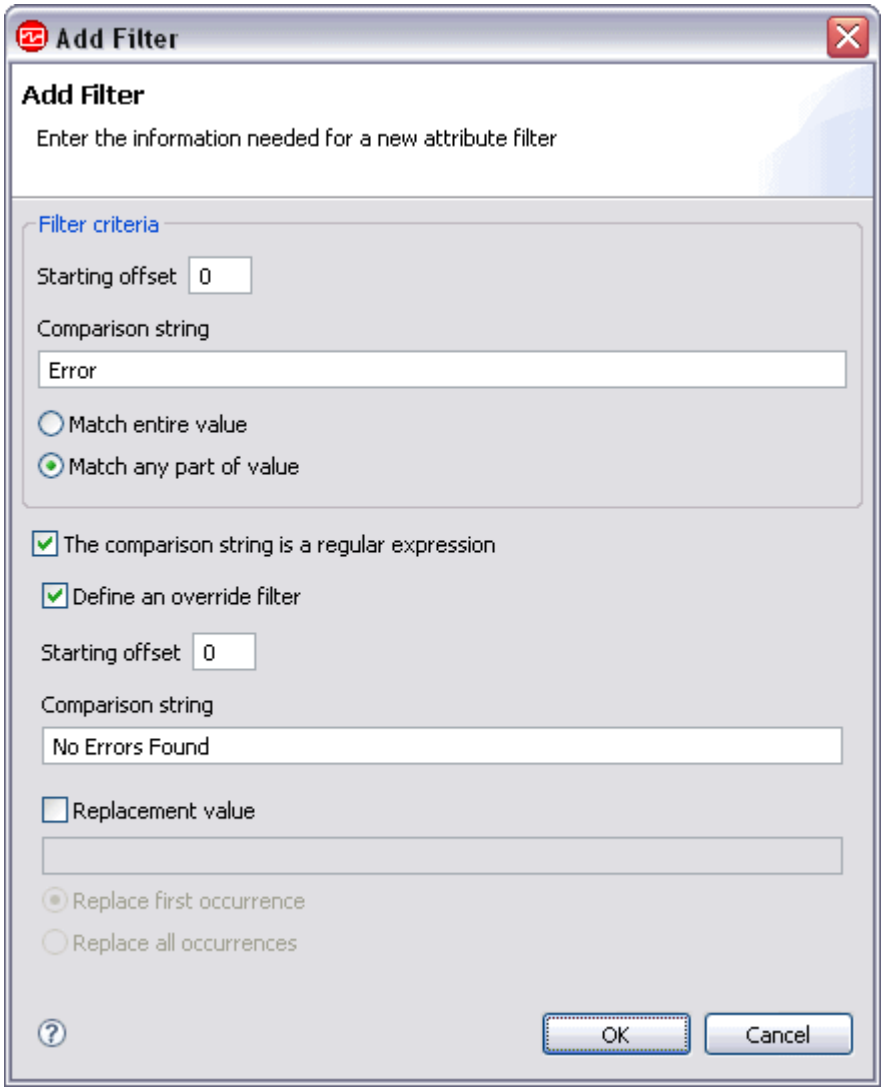


*Figura 39. Ejemplo 2 de **Añadir filtro***

Si la serie de atributo es `Error irrecuperable al leer el disco` y el filtro es **Inclusivo**, el atributo se muestra en el Tivoli Enterprise Portal o en la consola de IBM Cloud Application Performance Management. Si la serie de atributo es `No se han encontrado errores durante la copia de seguridad semanal` y el filtro es **Inclusivo**, no se visualiza el atributo.

d) En la sección **Identificación de campo** de la página **Información avanzada de atributo de archivo de registro**, especifique cómo alterar los delimitadores del campo de grupo de atributos solo para este atributo. Pulse uno de los filtros de atributo y complete los campos necesarios para la opción:

- **Número de caracteres**: Escriba el límite de número de caracteres.
- **Separador de separadores** especifica el uso de separadores en separadores.
- **Texto separador**: entre el texto separador que desea utilizar.
- **Texto inicial y final**: Escriba el texto **Inicial** y **Final**.

e) En la sección **Resumen** de la página **Información avanzada de atributo de archivo de registro**, pulse la casilla de verificación **Incluir atributo en grupo de atributos de resumen** para añadir el atributo al grupo de atributos de resumen.

Este grupo de atributos se genera cuando un usuario activa el resumen de atributos de registro.

f) Pulse **Aceptar**.

10. Si ha utilizado la función de prueba en el paso "7" en la página 1304, se visualiza la página **Seleccionar atributos clave**. En la página **Seleccionar atributos clave**, seleccione los atributos clave o indique que este origen de datos solo produce una fila de datos.

Para obtener más información, consulte ("Selección de atributos clave" en la página 1208).

11. Realice una de las acciones siguientes:

- Si utiliza el Asistente de agente nuevo, pulse **Siguiente**.
- Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.

Nota: Cuando se añade un grupo de atributos de archivo de registro a un agente con la versión mínima predeterminada de Tivoli Monitoring versión (6.2.1) o posterior, se incluye un grupo de atributos `Estado de archivo de registro`. Para obtener más información sobre el grupo de atributos `Estado de archivo de registro`, consulte "Grupo de atributos Estado del archivo de registro" en la página 1505.

Separadores y análisis de archivo de registro

Puede cambiar el separador predeterminado que se utiliza para separar uno o más atributos en un registro de archivo de registro.

Cuando crea un grupo de atributos de archivo de registro, se asigna un separador de forma predeterminada. El separador predeterminado es un separador. El agente utiliza el separador para analizar y delimitar los datos para cada atributo en la fila de datos. Puede cambiar el separador de atributo predeterminado para que sea:

- un número fijo de caracteres
- un espacio
- un carácter o caracteres diferentes
- un texto de comienzo y final específico
- un elemento XML.

Cambie el separador predeterminado que se utiliza para todos los atributos del grupo de las siguientes formas:

1. Cuando crea el grupo de atributos, en la página **Información de archivo de registro**.
2. Después de crear el grupo de atributos, abriendo el separador **Agent Editor** > **Orígenes de datos**, seleccionando el grupo de atributos y eligiendo un separador en el área **Identificación de campo**.

También puede asignar opcionalmente separadores específicos a uno o más atributos individuales. Puede asignar separadores específicos para que los atributos individuales utilicen:

- un número fijo de caracteres
- un separador de separadores
- un separador de espacios
- un carácter o caracteres diferentes
- un texto de comienzo y final específico.

Cambie el separador que se utiliza para atributos individuales de las siguientes formas:

1. Al seleccionar **Avanzado** en la página **Información de atributos** cuando crea un atributo.
2. Al abrir el separador **Agent Editor** > **Orígenes de datos**, seleccionar el atributo y seleccionar **Avanzado** en el separador **Información de atributos de archivo de registro**.

Ejemplo 1: salida de archivo de registro simple

Algunos archivos de registro tienen separadores claros y regulares, por ejemplo:

```
one,two,three
```

Aquí, el carácter " , " es un separador claro y regular entre los tres datos en la fila. En este caso, seleccione **Texto separador** y especifique " , " como el separador predeterminado para el grupo de atributos. No es necesario cambiar o definir otros separadores.

En la siguiente salida se muestra cómo definir este separador para un archivo de registro que contiene la fila de datos que se ha mostrado anteriormente en este ejemplo:

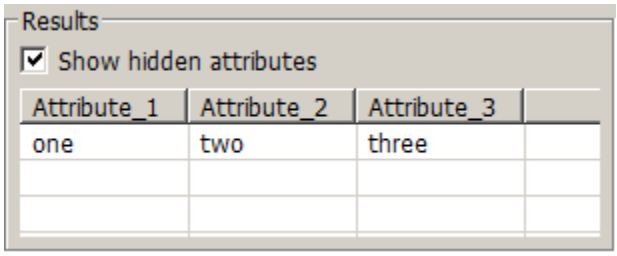


Figura 40. Salida de valor de atributo de ejemplo cuando el agente analiza una fila de datos de archivo de registro simple.

Ejemplo 2: salida de archivo de registro compleja

Algunos archivos de registro pueden contener filas de datos que tengan separadores cambiantes o irregulares, por ejemplo:

```
one,two,three,[four]12:42,five
```

En este ejemplo, una asignación de separadores para las definiciones de atributos que podría utilizar sería:

1. En el ejemplo anterior, establece el separador predeterminado en " , ". Este separador se utiliza para todos los atributos, a menos que lo altere temporalmente con un separador específico. En este ejemplo, el separador predeterminado de " , " es correcto para utilizarlo de nuevo para los primeros tres atributos de la fila.
2. Para el cuarto atributo, supongamos que la cadena entre "[" y "]" es un valor que desea extraer. En este caso, cuando defina el cuarto atributo, asigne un tipo de separador **Texto inicial y final** con los valores de texto inicial y final "[" y "]".
3. Para el quinto atributo, supongamos que desea extraer los valores entre los caracteres "]" y ":". En este caso, cuando defina el quinto atributo, asigne un tipo de separador **Texto separador** establecido en ":".
4. Para el sexto atributo, el separador de grupo de atributos predeterminado " , " es correcto nuevamente.
5. Para el séptimo atributo, no es necesario que especifique un separador ya que es el último atributo.

En la siguiente salida se muestra cómo definir estos separadores en un archivo de registro que contiene la fila de datos que se ha mostrado anteriormente en este ejemplo:

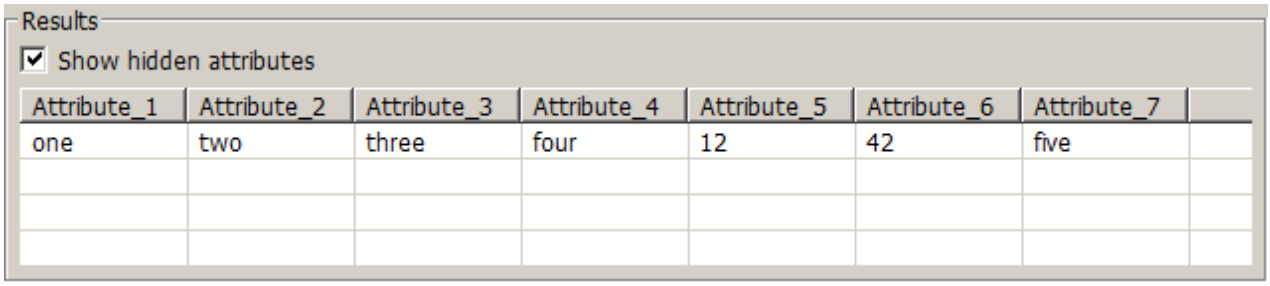


Figura 41. Salida de valor de atributo de ejemplo cuando el agente analiza una fila de datos de archivo de registro compleja.

El procedimiento para definir los separadores de atributo se describe bajo el paso "5" en la página 1300 de "Supervisión de un archivo de registro" en la página 1300.

Prueba de grupos de atributos de archivo de registro
Puede utilizar Agent Builder para probar el conjunto de datos del archivo de registro (grupo de atributos) que ha creado. Si no se han definido atributos para el grupo, el proceso de prueba los define automáticamente.

Antes de empezar
Si ya hay algún atributo definido para este conjunto de datos y desea definir atributos automáticamente durante la prueba, utilice el editor de agentes para eliminar los atributos existentes del conjunto de datos. Para obtener instrucciones, consulte "Eliminación de atributos" en la página 1233.

Procedimiento

1. El procedimiento de prueba se puede iniciar de las siguientes formas:
   - Durante la creación del agente, pulse **Probar valores de archivo de registro** en la página **Información de archivo de registro**.
   - Tras la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** y pulse **Valores del archivo de registro de prueba**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208.

   Después de pulsar **Probar valores de archivo de registro** en uno de los dos pasos anteriores, se abre la ventana **Analizar registro**.
2. Seleccione el origen de los datos de registro para la prueba:
   - **Utilizar valores de grupo de atributos**: utilice el nombre y la ubicación de archivo especificados en el origen de datos. De forma predeterminada, el origen de datos solo procesa la información que se añade al archivo de registro después de que se inicie el proceso de prueba. Puede utilizar esta opción si el archivo de registro se está actualizando en tiempo real.
   - **Especificar un archivo de ejemplo**: proporcione un archivo de registro de ejemplo. Con este valor, el procedimiento de prueba analiza todo el contenido del archivo de registro. Con esta opción, puede probar el origen de datos y crear los atributos para él inmediatamente, según un ejemplo existente. Especifique la vía de acceso y el nombre del archivo en el campo **Nombre de archivo de registro** o utilice el botón **Examinar** para seleccionar el archivo.
3. Opcional: Antes de empezar la prueba, puede establecer variables de entorno y propiedades de configuración.

   Para obtener más información, consulte ("Prueba de grupo de atributos" en la página 1417).
4. Pulse **Iniciar agente**.

   Se abre una ventana que indica que el agente se está iniciando. Cuando se inicia el agente, supervisa los nuevos registros del archivo de registro configurado.
5. Para probar la recopilación de datos del agente, genere nuevos registros en el archivo de registro supervisado.

Cuando se añaden nuevos registros al archivo de registro, el agente los analiza de acuerdo a su configuración y actualiza los valores de atributo correspondientes en su memoria caché.

6. Para simular una solicitud de Tivoli Enterprise Portal o SOAP para los datos de agente, pulse **Recopilar datos**.

   La ventana **Analizar registro** recopila y muestra los nuevos valores de atributo de la memoria caché del agente desde que se inició sesión por última vez. Puede ver un ejemplo de la recopilación de datos en Figura 42 en la página 1311

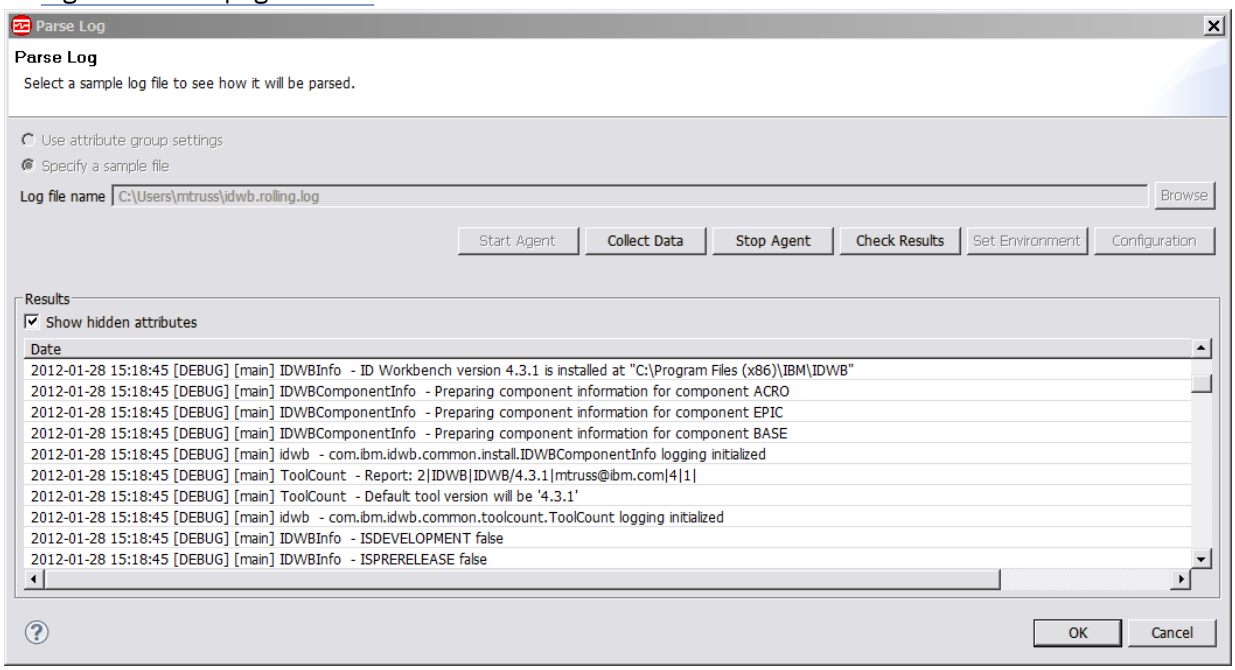


Figura 42. Ventana Analizar registro que muestra valores de atributos de archivo de registro analizados

7. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana Estado de la recopilación de datos recopila y muestra se describen en "Nodo Estatus de objeto de rendimiento" en la página 1462

8. El agente se puede detener pulsando **Detener agente**.
9. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Analizar registro**. Al pulsar **Aceptar** se guardan los cambios que ha realizado.

Conceptos relacionados

"Pruebas del agente en Agent Builder" en la página 1417
Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión de un registro binario de AIX

Puede definir un origen de datos para supervisar registros de errores binarios de AIX mediante el mandato `errpt`. También puede configurarlo para filtrar y resumir los datos. Los sucesos resultantes se colocan en un conjunto de datos.

Acerca de esta tarea

La supervisión de registros soporta la supervisión de registros de errores binarios de AIX mediante el mandato `errpt`. El mandato `errpt` genera un informe de error de las entradas en un registro de error. Incluye distintivos para la selección de errores que coinciden con criterios específicos. Este soporte para la supervisión de registros de error binarios de AIX mediante el mandato `errpt` es modelado en el soporte para la misma función en el Tivoli Monitoring UNIX Logs Agent (código de producto `kul` o `ul`).

Cuando proporcione a Agent Builder una cadena de mandato **`errpt`**, procesará los sucesos que resulten de la ejecución de este mandato. Agent Builder impone las mismas restricciones sobre este mandato que

el Monitoring Agent for registros de UNIX. En particular, debe utilizar la opción **-c** (modalidad simultánea) para que el mandato se ejecute continuamente y no puede utilizar la opción **-t** o las siguientes opciones que tiene como resultado una salida detallada: **-a**, **-A** o **-g**.

Un agente Agent Builder que supervisa el mandato AIX **errpt** automáticamente incluye la misma información que el Monitoring Agent for registros de UNIX. Para obtener información sobre los grupos de atributos para los registros de error binarios de AIX, consulte "Grupo de atributos de registro binario de AIX" en la página 1476.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos registrados** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse en **Registro binario de AIX**.
3. Pulse **Siguiente**.
4. En la página **Información de registro binario**, especifique un mandato `errpt`.

   El valor predeterminado es:

   ```
   errpt -c -smmddhhmmyy
   ```

   El agente busca la cadena 'mmddhhmmyy' y la sustituye por la fecha y la hora real durante el inicio. Solo se sustituye la primera aparición de la cadena.

   Puede proporcionar su propio mandato `errpt` pero Agent Builder impone las mismas restricciones en este mandato que el Monitoring Agent for los registros de UNIX. En particular, debe utilizar la opción **-c** (modalidad simultánea) para que el mandato se ejecute continuamente y no puede utilizar la opción **-t** o las siguientes opciones que tiene como resultado una salida detallada: **-a**, **-A** o **-g**.
5. (Opcional) Pulse **Avanzado** para seleccionar las opciones de filtrado y resumen para sucesos. Para obtener más información, consulte "Control de sucesos duplicados" en la página 1446.
6. Realice una de las acciones siguientes:
   - Si utiliza el **Asistente de agente**, pulse **Siguiente**.
   - Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.

Referencia relacionada

"Grupo de atributos de registro binario de AIX" en la página 1476
El grupo de atributos de registro binario de AIX muestra sucesos del registro binario de AIX tal como lo ha seleccionado la cadena de mandato `errpt`.

Supervisión de un registro de sucesos de Windows

Puede definir un origen de datos para recopilar datos de un registro de sucesos Windows. Puede configurarlo para filtrar los datos. Los sucesos resultantes se colocan en un conjunto de datos Registro de sucesos.

Acerca de esta tarea

Puede recopilar datos del registro de sucesos de Windows utilizando el tipo, el origen o el ID de los sucesos. Se utilizan estos parámetros para filtrar los sucesos de registro que el sistema Windows ha recopilado. El agente compara todos los sucesos nuevos del registro de sucesos supervisados con el filtro especificado. El suceso se pasará si coincide con uno de los tipos de sucesos, orígenes de suceso o ID de suceso especificados.

Por ejemplo, si el filtro del registro de sucesos es para el registro de aplicaciones, especifique **Error** como tipo de suceso. Esta opción coincide con todos los sucesos que se han registrado en el registro de aplicaciones con un valor de tipo de suceso de `error`. Si añade los orígenes de sucesos **Diskeeper** y **Symantec AntiVirus**, el agente buscará coincidencias con todos los sucesos de error de ambos orígenes. Si desea aportar mayor precisión al filtro, puede añadir ID de sucesos específicos. No existe ninguna asociación directa entre el tipo de suceso, el origen del suceso y el ID del suceso. Si uno de los valores de uno de ellos coincide con un suceso, el suceso coincidirá.

De forma predeterminada, solo se procesan los sucesos que se generan después de que el agente se inicia. Sin embargo, puede habilitar el agente cuando vuelva a procesar sucesos de registro que se generen mientras el agente no se cierra. Si desea más información sobre cómo habilitar el agente para procesar sucesos generados mientras el agente está cerrado, consulte el paso "6" en la página 1313.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos registrados** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse en **Registro de sucesos de Windows**.
3. Pulse **Siguiente**.
4. En la página **Registro de sucesos de Windows**, seleccione el nombre de uno de los registros en la lista **Nombre de registro de sucesos de Windows**, o escriba el nombre de un registro de sucesos.

   La lista se crea a partir el conjunto de registros del sistema actual, por ejemplo:

   ```
   Aplicación
   Seguridad
   Sistema
   ```
5. En la página **Registro de sucesos de Windows**, especifique si desea filtrar los resultados utilizando uno o más de los mecanismos siguientes:

   - "Filtrado por tipo de suceso" en la página 1314
   - "Filtrado por origen de sucesos" en la página 1314
   - "Filtrado por identificador de suceso" en la página 1315

   Nota: Como mínimo debe seleccionar uno de estos criterios de filtro.
6. Para procesar los sucesos de registro que se generan mientras el agente está cerrado, en un reinicio del agente, pulse **Valores de suceso fuera de línea** en la página **Registro de sucesos de Windows**.

   Se abre la ventana **Valores de marcador de registro de sucesos de Windows**.
7. Seleccione una de las siguientes opciones de marcadores:

   Nota: Estas opciones se aplican a todos los registros de suceso de Windows que se están supervisando.

   - **No recopile sucesos fuera de línea**: los sucesos que se generan mientras el agente está cerrado no se procesan. Esta opción es la opción predeterminada.
   - **Recopile todos los objetos fuera de línea**: todos los sucesos que se generan mientras el agente está cerrado se procesan.
   - **Especifique valores de recopilación personalizados**: puede especificar un valor para regular el proceso de sucesos antiguos que están basados en un valor de hora, en un número de sucesos o en ambos. Utilizando esta opción, se asegura de que el entorno de supervisión no está sobrecargado con sucesos cuando se inicia el agente.

     Por ejemplo, si se ha entrado 100 en el campo **Número máximo de sucesos para recopilar** y 30 en el campo **Restringir recopilación según un intervalo de tiempo (en segundos)**. El número de sucesos que se procesan es los 100 últimos sucesos que se generan antes de que el agente se inicie, o cualquier suceso que se genere en los 30 segundos siguientes al inicio del agente. El resultado depende de la variable que coincide primero.

     Cuando entra un valor para el número máximo de sucesos que se deben recopilar, se añade la variable de entorno *CDP_DP_EVENT_LOG_MAX_ BACKLOG_EVENTS*. Cuando especifica un valor para restringir la recopilación basada en un intervalo de tiempo, se añade la variable de entorno *CDP_DP_EVENT_LOG_MAX_BACKLOG_TIME*. Cuando se añade una variable o ambas, se crea el archivo *nombre_registro_sucesos_código_producto_nombre_instancia_nombre_subnodo*`.rst` que contiene el último registro de sucesos procesado para el registro de sucesos. Este archivo se encuentra en el directorio *%CANDLE_HOME%*`\tmaitm6\logs` y se utiliza cuando el agente se

reinicia para procesar los sucesos antiguos que se han generado mientras el agente estaba cerrado.

8. Si desea establecer opciones globales para el origen de datos, pulse **Opciones globales** en la página **Registro de sucesos de Windows**

   Se abre la ventana **Opciones globales de origen de datos de Windows**.

9. Seleccione el recuadro de selección **Incluir propiedades de configuración de Windows remoto** si desea incluir esta opción y pulse **Aceptar**.

   Si desea más información sobre la configuración de conexión remota de Windows para orígenes de datos de Windows, consulte "Configuración de una conexión remota de Windows" en la página 1404.

10. Después de especificar el filtro y pulsar **Aceptar**, en la página **Registro de sucesos de Windows**, realice uno de los pasos siguientes:
    - Si utiliza el **Asistente de agente**, pulse **Siguiente**.
    - Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor. El nombre del nuevo registro de sucesos de Windows se muestra en la página **Definición de origen de datos** de **Agent Editor**.

Qué hacer a continuación

Para obtener información sobre la configuración de conexión al sistema Windows remoto para fuentes de datos del registro de sucesos de Windows, consulte "Configuración de una conexión remota de Windows" en la página 1404.

Filtrado por tipo de suceso
Filtre los resultados del registro de sucesos de Windows por tipo de suceso

Procedimiento

1. En la página **Registro de sucesos de Windows**, seleccione **Filtrar por tipo de suceso**.
2. Seleccione uno o más de los siguientes tipos de sucesos:
   - **Información**
   - **Aviso**
   - **Error**
   - **Auditoría satisfactoria**
   - **Auditoría de fallos**
3. Pulse **Finalizar** para terminar.

Filtrado por origen de sucesos
Filtre los resultados del registro de sucesos de Windows por origen de sucesos

Procedimiento

1. Seleccione **Filtrar por origen de suceso** y pulse **Añadir** en el área **Orígenes de sucesos** de la página **Registro de sucesos de Windows**.

   Se abre la ventana **Origen de sucesos**.

2. Realice una de las siguientes selecciones.
   - Escriba el nombre del origen de sucesos y pulse **Aceptar**.
   - Pulse **Examinar** para buscar y seleccionar un origen de suceso en una lista y pulse **Aceptar**.

     El nombre que ha seleccionado se muestra en la ventana **Origen de sucesos**.

     Nota:

     a. Para ordenar la lista de orígenes de sucesos, pulse la cabecera de columna.
     b. Para renovar la información de la ventana, pulse en el icono **Renovar**.

c. Para buscar orígenes de sucesos específicos, pulse el icono **Buscar** (binoculares).

3. Pulse **Aceptar** para ver el nuevo filtro de origen de sucesos en la lista de orígenes Orígenes de sucesos en la ventana **Registro de sucesos de Windows**.

Filtrado por identificador de suceso
Para el origen de datos del registro de sucesos de Windows, puede filtrar los sucesos por identificador de suceso.

Acerca de esta tarea

Para filtrar por identificador de suceso, utilice el procedimiento siguiente:

Procedimiento

1. Seleccione **Filtrar por identificador de sucesos** y pulse **Añadir** en el área **Identificadores de sucesos** de la ventana **Registro de sucesos de Windows**.

   Se abre la ventana **Identificador de sucesos**.
2. Si conoce los sucesos específicos que desea supervisar de una aplicación, especifique los números de los sucesos tal como los define la aplicación. Escriba un número entero como identificador del suceso y pulse **Aceptar**.

   El nuevo filtro de identificador de sucesos numérico se muestra en la lista Identificadores de sucesos en el **Registro de sucesos de Windows**.

   Nota: Cada identificador de suceso debe definirse individualmente.
3. Si desea modificar un registro de suceso de Windows, selecciónelo y pulse **Editar**.
4. Si desea suprimir un registro de suceso de Windows, selecciónelo y pulse **Eliminar**.
5. Puede añadir más registros de suceso a la lista o pulsar en **Finalizar**.

Supervisión de un código de retorno de mandato

Puede definir un origen de datos para supervisar una aplicación o un sistema utilizando un *código de retorno de mandato*. El agente ejecuta el mandato, recopila el código de retorno y añade el resultado al conjunto de datos de Disponibilidad.

Acerca de esta tarea

Un script creado por el usuario, archivo ejecutable, consulta o mandato del sistema puede devolver un código. Un código de retorno de mandato es un mecanismo específico de aplicación para determinar si la aplicación o el sistema supervisado están disponible. El agente ejecuta el mandato especificado y determina el estado de la aplicación o el sistema supervisado examinando el código de retorno.

El mandato debe presentar un código de retorno exclusivo para cada estado descriptivo. El mandato también debe definir un mensaje que el agente debe utilizar para cada uno de estos códigos de retorno. El mandato puede utilizar variables de entorno y configuración dentro del script creado por el usuario, el archivo ejecutable, la consulta o el mandato del sistema. El mandato no debe utilizar variables de entorno ni de configuración en la invocación del mandato en línea de mandatos, y solo tendrá disponibles las siguientes excepciones: *AGENT_BIN_DIR*, *AGENT_ETC_DIR*, *AGENT_LIB_DIR*, *CANDLE_HOME* y *CANDLEHOME*.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, seleccione **Mandato o script** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **Código de retorno de un mandato**.
3. Pulse **Siguiente**.
4. En la página **Código de retorno de mandato**, área **Información de código de retorno de mandato**, escriba el nombre de visualización.

5. Utilice los subpasos siguientes para definir y describir las líneas de mandato que desea que el código de retorno de mandato utilice.

   Nota: Defina un mandato para cada sistema operativo soportado por el agente. Los mandatos se pueden compartir, pero el conjunto total de sistemas operativos para todos los mandatos debe ser igual al conjunto de sistemas operativos soportados por el agente.

   a) Pulse **Añadir** en el área **Mandatos** de la ventana **Código de retorno de mandato** para abrir la ventana **Información de mandato**.

   b) Escriba una línea de mandatos y seleccione un sistema operativo en la lista del área **Sistemas operativos** de la ventana **Información de mandato**.

      Nota:

      1) Para un mandato de Windows, es necesario escribir el nombre completo del mandato. Por ejemplo, `mandato_que_se_ejecutará.bat` y no solo `mandato_que_se_ejecutará`.
      2) Especifique el nombre entre comillas para que el intérprete de mandatos no lo analice. Por ejemplo, escriba `"esto es una prueba.bat"argumento` y o `esto es una prueba.bat argumento`.
      3) Puede pulsar en un mandato y a continuación en **Editar** para modificarlo o pulsar en **Eliminar** para suprimirlo.

   c) Pulse **Añadir** en el área **Códigos de retorno** de la ventana **Información de mandato**.

   d) Seleccione un tipo de código de retorno en la lista que se muestra en la ventana **Definición de código de retorno**

      Puede asignar los estados siguientes a los códigos de retorno de la prueba:

      - `YA EN EJECUCIÓN`
      - `DEPENDIENTE NO EN EJECUCIÓN`
      - `ERROR GENERAL`
      - `NO EN EJECUCIÓN`
      - `CORRECTO`
      - `REQUISITO PREVIO NO EN EJECUCIÓN`
      - `AVISO`

   e) Escriba un valor numérico para el tipo de código de retorno que ha seleccionado.

      El valor del código de retorno es un número entero que especifica un código de retorno definido para el código de retorno del mandato. Por motivos de probabilidad entre sistemas operativos, utilice un valor de código de retorno de `0 - 255`. Para un mandato que solo se ejecuta en Windows, el valor del código de retorno puede ser `-2147483648 - 2147483647`.

   f) Defina un mensaje para cada código de retorno para que el mensaje y el código se puedan mostrar juntos. Pulse en **Examinar** para configurar el texto del mensaje.

      La ventana de mensajes muestra una lista de los mensajes que están definidos en el agente. Se abre la ventana **Mensajes** (lista).

      Nota:

      1) Puede seleccionar texto que se haya especificado previamente seleccionándolo en la lista de textos de mensaje, en lugar de pulsando **Examinar**. Después, continúe al Paso 5k.
      2) Hasta que defina mensajes, la lista permanece en blanco. Puede utilizar **Editar** para alterar un mensaje definido y **Eliminar** para suprimir uno o más mensajes que ha definido.

   g) En la ventana **Mensajes** (lista), pulse **Añadir**

      Se abre la ventana **Definición de mensaje**.

      Nota: El identificador de mensaje se generará de forma automática.

   h) Escriba un texto que describa el significado del mensaje nuevo en el campo **Texto del mensaje**.

i) Pulse **Aceptar**.

La ventana **Mensajes** (lista) se abre y muestra el nuevo mensaje.

j) Para verificar el mensaje y convertirlo en permanente, selecciónelo en la lista y pulse **Aceptar**.

El nuevo tipo de código de retorno, el valor y el texto se visualizan en la ventana **Definición de código de retorno**.

k) Si desea que este código de retorno esté disponible para otros mandatos de otros sistemas operativos para este código de retorno del mandato, seleccione **El código de retorno global se aplica a todos los mandatos**. Si desea que este código de retorno solo esté disponible para este mandato, deje seleccionada la opción **El código de retorno local solo se aplica a este mandato**.

l) Pulse **Aceptar** en la ventana **Definición de código de retorno**.

m) Defina al menos dos códigos de retorno antes de salir de la ventana **Información de mandato**. Un código de retorno para indicar que no hay problemas con la disponibilidad, otro para indicar que se ha producido un problema. Si desea añadir otro código de retorno, vuelva al paso c.

n) Opcional: En la ventana **Información de mandato**, el área **Archivos de mandato**, pulse **Añadir** si desea seleccionar uno o más scripts o archivos ejecutables para que los ejecute el agente.

El archivo o archivos se copian en la carpeta del proyecto del agente en `scripts/`*`sistema operativo`*, donde *sistema operativo* es una variable que depende de lo que haya seleccionado en el área **Sistemas operativos** de la ventana **Información de mandato**. Estos archivos también se empaquetan y se distribuyen con el agente. Para editar la definición de un archivo de mandatos existente, o el archivo de mandatos original desde que se copió en el proyecto, seleccione el archivo y pulse **Editar**. Consulte ("Edición de una definición de archivo de mandatos" en la página 1318).

o) Pulse **Aceptar** en la ventana **Información de mandato**.

Nota: La tabla de archivos de mandatos es donde debe definir los archivos externos que desee incluir en el paquete del agente. Estos archivos se copian en el directorio del proyecto y se empaquetan con el agente para su distribución.

6. Si tiene otros códigos de retorno que aún no se han definido, defina y describa códigos de retorno globales que el código de retorno de mandato pueda utilizar.

a) Pulse **Añadir** en el área **Códigos de retorno globales** de la página **Código de retorno de mandato**.

Nota: Los códigos de retorno que se definen aquí son globales. Esto significa que los códigos de retorno son adecuados para todos los mandatos definidos para el código de retorno de mandato. (No se comparten entre códigos de retorno de mandatos). Además, puede definir códigos de retorno cuando especifique la información del mandato. Los códigos de retorno aquí definidos pueden ser globales o locales. Los códigos de retorno locales solo resultan adecuados para este mandato específico. Esta jerarquía resulta útil si un código de retorno es el mismo en todos los sistemas operativos. (Por ejemplo, un código de retorno de 0 significa que todo funciona correctamente. Puede definirlo a nivel global y, a continuación, todos los mandatos definidos interpretan 0 de esta manera). Si ninguno de los demás sistemas operativos devuelve 5, puede definir el código de retorno 5 solo para el mandato de Windows. Si define un código de retorno a nivel de mandato local que ya está definido a nivel global, se utiliza el nivel de mandato. Puede utilizar este método para sustituir los códigos de retorno de sistemas operativos específicos. Por ejemplo, si en todos los sistemas operativos UNIX, un código de retorno de 2 tiene un significado, pero en Windows tiene otro. Puede definir el código de retorno 2 a nivel global tal como esperan los sistemas operativos UNIX. Entonces, en el mandato para Windows, puede volver a definir el código de retorno 2 para proporcionarles un valor en Windows.

b) Seleccione un tipo de código de retorno en la lista que se muestra en la ventana **Definición de código de retorno**.

Puede asignar los estados siguientes a los códigos de retorno de la prueba:

- `YA EN EJECUCIÓN`
- `DEPENDIENTE NO EN EJECUCIÓN`
- `ERROR GENERAL`

- NO EN EJECUCIÓN
- Aceptar
- REQUISITO PREVIO NO EN EJECUCIÓN
- AVISO

c) Escriba un valor numérico para el tipo de código de retorno que ha seleccionado. El valor del código de retorno es un número entero que especifica un código de retorno definido para el código de retorno del mandato.

d) Pulse **Examinar** para configurar el texto del mensaje y el significado asociado al mismo. Debe definir un mensaje para cada código de retorno para que el mensaje y el código se muestren juntos.

La ventana **Mensajes** lista los mensajes definidos en el agente.

Nota:

1) Hasta que defina mensajes, la lista permanece en blanco. Puede utilizar **Editar** para alterar un mensaje definido y **Eliminar** para suprimir uno o varios mensajes que ha definido.
2) Puede seleccionar texto que se ha entrado previamente seleccionándolo en la lista **Texto de mensaje** en lugar de pulsar **Examinar**. Después, continúe con el Paso 6h.

e) En la ventana **Mensajes** (lista), pulse **Añadir** para ver la ventana **Definición de mensaje**, donde puede escribir texto que describa el significado del nuevo mensaje.

f) Pulse **Aceptar**.

g) Se abre la ventana **Mensaje** (lista) con el nuevo mensaje. Para verificar el mensaje y convertirlo en permanente, selecciónelo en la lista y pulse **Aceptar**.

h) Cuando se muestran el texto, tipo y valor nuevos en la ventana **Definición de código de retorno**, pulse **Aceptar**.

i) En la página Código de retorno del mandato, cuando haya terminado de definir los códigos de retorno y los mandatos para todos los sistemas operativos soportados, siga uno de los pasos siguientes:

- Si utiliza el Asistente de agente nuevo, pulse **Siguiente** o pulse **Finalizar** para guardar el origen de datos y abrir Agent Editor.
- Si utiliza el Asistente del nuevo agente, pulse **Finalizar** para volver a Agent Editor.

Qué hacer a continuación

Si desea utilizar los datos de este origen de datos en el panel de instrumentos de resumen para IBM Cloud Application Performance Management, debe crear un conjunto de datos filtrados (grupo de atributos) basado en el conjunto de datos de disponibilidad y configurarlo para proporcionar una sola fila. Utilice el campo NOMBRE para seleccionar la fila para su proceso.

En el grupo de atributos filtrados nuevo, seleccione el campo Estado y especifique los valores de gravedad para él.

Para obtener instrucciones consulte:

- “Creación de un grupo de atributos filtrado” en la página 1382
- “Especificar la gravedad de un atributo utilizado como indicador de estado” en la página 1238
- “Preparación del agente para Cloud APM” en la página 1414

Edición de una definición de archivo de mandatos

Puede cambiar el archivo de mandatos que se importa al proyecto o importar cambios al archivo de mandatos existente en el proyecto.

Procedimiento

1. Seleccione el archivo en el área **Archivos de mandatos** de la ventana **Información de mandato**.
2. Pulse **Editar** para abrir la ventana **Importar archivo de mandatos**.

En la ventana **Importar archivo de mandatos**, puede obtener el estado del archivo de mandatos. También puede cambiar la ubicación del archivo de origen original, y volver a copiar el archivo de origen en el agente.

3. Elija uno de los pasos siguientes:
   - Pulse **Aceptar** para planificar que se realice una copia del archivo la próxima vez que se guarde el agente.
   - Pulse **Copiar inmediatamente** para copiar el archivo sin guardar primero el agente.

   Nota: La opción **Copiar inmediatamente** no está disponible cuando se accede a la ventana **Importar archivo de mandatos** desde el Asistente de agente nuevo.

Separación y consolidación de archivos

Puede utilizar las funciones Separar y Consolidar para mover los archivos a las carpetas específicas del sistema operativo o fuera de ellas en el agente.

Cuando se añade un archivo por primera vez al agente, se añade una única copia a la carpeta `scripts/all_windows`, la carpeta `scripts/all_unix` o la carpeta `scripts/common`. La carpeta `scripts/common` se utiliza si el archivo se usa en Windows y UNIX.

Para colocar distintas copias del archivo en distintos sistemas operativos (por ejemplo, un archivo ejecutable binario), pulse **Editar** y **Separar**. El archivo se elimina de la carpeta común y se copia en carpetas específicas del sistema operativo. A continuación, puede sustituir las copias individuales del archivo por las adecuadas para los sistemas operativos específicos.

Nota: Los archivos de recursos de Java deben permanecer en la carpeta `scripts/common`. No puede pulsar **Separar** para hacer copias independientes de los archivos de recursos de Java para sistemas operativos individuales.

Si ha separado los archivos en carpetas de sistema operativo, puede utilizar **Consolidar** para devolverlos a una carpeta común. Si ha creado el agente en una versión de Agent Builder que no soportaba carpetas comunes, utilice **Consolidar** para devolverlos a una carpeta común. Si alguna de las copias del archivo difiere de la otra, se le solicitará que seleccione el archivo que se debe utilizar como archivo común. Todas las demás copias se descartan.

Supervisar salida de un script

Puede definir un origen de datos para recopilar los datos de un script o de un programa externo. Utilícelo si los datos de aplicación no están disponibles a través de una interfaz de gestión estándar o si tiene que proporcionar un resumen de datos de varias filas en una sola fila. El agente ejecuta el script y recopila la salida. Cada línea de la salida del script se analiza en una fila del conjunto de datos resultante.

Los datos se pueden recopilar desde un sistema local o remoto. La salida del script o el programa solo debe contener valores para cada atributo dentro del grupo de atributos. Para devolver varias filas de datos, los datos para cada fila deben estar separados por un salto de línea. Los atributos de cada fila de datos están separados por los separadores que defina. Para obtener más información sobre separadores, consulte “Separadores y análisis de script” en la página 1320

El mandato puede utilizar variables de configuración y entorno dentro del script creado por el usuario, archivo ejecutable, consulta o mandato del sistema. El mandato no puede utilizar variables de configuración ni entorno en la invocación de la línea de mandatos, y solo tendrá disponibles las siguientes excepciones: `AGENT_BIN_DIR`, `AGENT_ETC_DIR`, `AGENT_LIB_DIR`, `CANDLE_HOME` y `CANDLEHOME`.

La salida de script de supervisores de agente que se escribe utilizando el mismo entorno local y página de códigos donde se ejecuta el agente.

Recopilación de datos de script de un sistema remoto

Para recopilar datos de script o de programa de un sistema remoto, Agent Builder utiliza Secure Shell (SSH)

Para recopilar datos de un sistema remoto, Agent Builder crea una sesión de Secure Shell (SSH) e inicia el script o el programa externo en el sistema remoto. El agente se establece y se conecta a una sesión SSH. A continuación, el agente carga los scripts en el sistema remoto, inicia el script o el programa externo y

recupera la salida. El agente se puede configurar para mantener la sesión abierta o volver a establecer la sesión para cada invocación. Si la sesión se mantiene abierta, el script se puede reutilizar o cargar para cada invocación. De forma predeterminada, se utiliza una sola sesión de SSH y los scripts se reutilizan para cada invocación.

Agent Builder solo soporta la utilización del protocolo SSH versión 2 con las claves RSA (Rivest, Shamir y Adleman) o DSA (algoritmo de firma digital). El agente es autenticado mediante el nombre de usuario y la contraseña, o mediante una autenticación de clave pública. La generación y distribución de las claves públicas es una tarea administrativa que debe realizarse fuera del agente y Agent Builder.

Para ejecutar un mandato de Actuación escrito sobre un proveedor de datos de script habilitado de Secure Shell (SSH) en el sistema remoto, consulte “Acción SSHEXEC” en la página 1547.

Restricción: Si el agente se ha creado con una versión de Agent Builder anterior a 6.3 y tiene un proveedor de datos de script que utiliza SSH, el proveedor fallará al ejecutarse con IBM Tivoli Monitoring versión 6.3 o posterior. Para resolver este problema, vuelva a crear el agente con la versión actual de Agent Builder.

La restricción se debe a que IBM Tivoli Monitoring versión 6.3 utiliza una versión más reciente de la API de Global Secure ToolKit (GSKit). Debe volver a crear el agente con Agent Builder 6.3 o posterior para ejecutarlo IBM Tivoli Monitoring versión 6.3 o posterior. Si crea el agente con Agent Builder 6.3, también se puede ejecutar con versiones anteriores de IBM Tivoli Monitoring.

Separadores y análisis de script

Puede cambiar y asignar separadores de script específicos a uno o varios atributos.

Cuando se crea un grupo de atributos de script, se asigna de forma predeterminada un único separador de texto de caracteres. El separador predeterminado es " ; ". El agente utiliza el separador para analizar y delimitar los datos para cada atributo en la fila de datos. Puede cambiar el separador predeterminado para utilizar un carácter diferente. También puede asignar separadores específicos a uno o más atributos individuales.

Puede asignar separadores específicos para atributos individuales que:

- Tomen un número fijo de bytes de la salida.
- Separen un atributo del siguiente con un separador personalizado, que puede ser más de un carácter.
- Delimiten un valor de atributo con una cadena al principio y al final del valor.
- Devuelvan el resto del texto como el valor de atributo (tanto si contiene separadores incorporados como si no).

Puede utilizar uno o más de estos separadores para extraer valores de atributo de las filas de datos.

Ejemplo 1 - Salida de script simple

Algunos scripts pueden generar filas de datos con separadores claros y habituales, por ejemplo:

```
Fila uno;1;2
Fila dos;3;4
Fila tres;5;6
```

Aquí, el carácter " ; " es un separador claro y habitual entre trozos de datos en cada fila. En este caso, el separador predeterminado está bien, por lo que no es necesario cambiar o definir otros separadores. No es difícil imaginar una salida de script similar en la que el separador sea un carácter diferente, como en el siguiente ejemplo.

```
Fila uno-1-2
Fila dos-3-4
Fila tres-5-6
```

En este ejemplo, se ha cambiado el carácter separador " ; " por el carácter " - ". En este caso, cuando defina los atributos, cambie el separador predeterminado para utilizar el carácter " - ".

Ejemplo 2 - Salida de script compleja

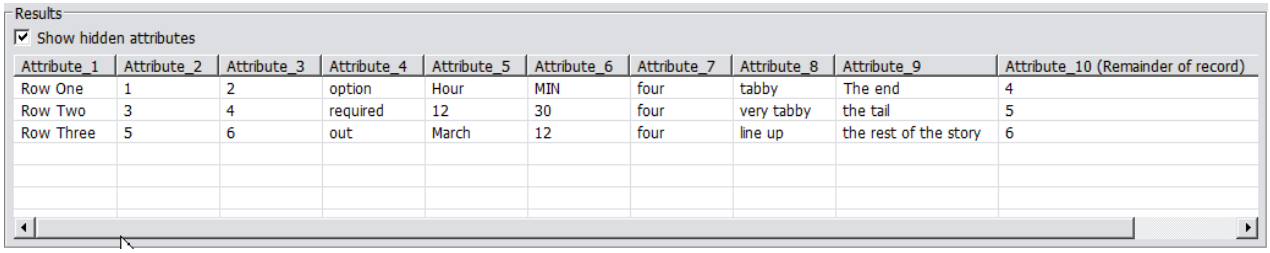
Algunos scripts pueden producir filas de datos de salida que tengan separadores irregulares o cambiantes, por ejemplo:

```
Row One;1;2;[option]Hour:MIN;fourtabby     The end;4
Row Two;3;4;[required]12:30;fourvery tabby the tail;5
Row Three;5;6;[out]March:12;fourline up    the rest of the story;6
```

En este ejemplo, una asignación de separadores para las definiciones de atributos que podría utilizar sería:

1. Inicialmente, el separador predeterminado "`;`" es bueno para los tres primeros atributos de cada fila de datos. En este caso, asigne el tipo de separador **Texto separador** establecido en "`;`" cuando defina cada atributo, este es el valor predeterminado.
2. Para el cuarto atributo, supongamos que la cadena entre "`[`" y "`]`" es un valor que desea extraer. En este caso, cuando defina el cuarto atributo, asigne un tipo de separador **Texto inicial y final** con los valores de texto inicial y final "`[`" y "`]`".
3. Para el quinto atributo, supongamos que desea extraer los valores entre los caracteres "`]`" y "`:`". En este caso, cuando defina el quinto atributo, asigne un tipo de separador **Texto separador** establecido en "`:`".
4. Para el sexto atributo, el separador predeterminado "`;`" está bien, acepte el predeterminado.
5. Para el séptimo valor, le gustaría extraer la cadena en los siguientes cuatro caracteres "`four`". No hay ningún separador claro al final de esta cadena. Puede asignar un número de caracteres para definir la separación del siguiente atributo. Asigne un tipo de separador **Número de caracteres**, y especifique cuatro caracteres como la longitud.
6. Para el octavo atributo, le gustaría extraer las cadenas `tabby`, `very tabby` y `line up`. En este caso, supongamos que todas estas cadenas van seguidas por el carácter de tabulación. En este caso, asigne un tipo de separador **Separador de separadores**.
7. Para el noveno atributo, revierta de nuevo al tipo de separador predeterminado para extraer el resto del texto a este atributo.
8. Para el décimo atributo, especifique **Resto del registro** para asignar el resto de la fila de datos a este atributo.

En la salida siguiente se muestra cómo definir estos separadores en un script que produce las filas de datos mostradas anteriormente en este ejemplo:


Results

Show hidden attributes

Attribute_1	Attribute_2	Attribute_3	Attribute_4	Attribute_5	Attribute_6	Attribute_7	Attribute_8	Attribute_9	Attribute_10 (Remainder of record)
Row One	1	2	option	Hour	MIN	four	tabby	The end	4
Row Two	3	4	required	12	30	four	very tabby	the tail	5
Row Three	5	6	out	March	12	four	line up	the rest of the story	6

Figura 43. Salida de valor de atributo de ejemplo cuando el agente analiza una salida de script compleja.

El procedimiento para definir los separadores de atributo se describe bajo el paso “10” en la página 1324 de “Pasos para supervisar la salida de un script” en la página 1321.

Pasos para supervisar la salida de un script

Configure el agente para que reciba datos de un origen de datos de script.

Antes de empezar

Consulte “Supervisar salida de un script” en la página 1319

Acerca de esta tarea

Utilice el procedimiento siguiente para supervisar la salida de un script:

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, seleccione la opción **Mandato o script** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **Salida de un script**.
3. Pulse **Siguiente**.
4. En la página **Lista de mandatos**, pulse **Añadir** para visualizar una ventana **Información de mandato**.

   Nota: Al marcar el recuadro de selección **Habilitar la recopilación de datos utilizando SSH** se habilita SSH para este grupo de atributos. Si este recuadro de selección no está seleccionado, el grupo de atributos se ejecuta de forma local.

   Nota: Si existe un mandato que pueda ejecutarse en el sistema operativo en el que Agent Builder se está ejecutando, se habilita la opción **Probar**. Puede utilizar **Probar** para probar un mandato que haya definido.
5. En el área **Información de mandato** en la ventana **Información de mandato**, escriba un nombre de mandato con los argumentos necesarios en el campo **Mandato** y un separador en el campo **Separador**.

   Nota:

   a. Los scripts de Windows se inician con frecuencia sin especificar la extensión `.bat` o `.cmd` en la línea de mandatos. Para la ejecución remota, debe instalarse un entorno de shell y se debe especificar `.bat` o `.cmd` en el mandato de origen de datos de script para que se ejecute el script. `Cygwin` es un ejemplo de entorno de shell que está disponible para Windows. Linux, Red Hat y AIX. Para verificar que existe un entorno de shell, SSH o inicie sesión en el host remoto y especifique el mandato:

   ```
   PATH=$PATH:. <mandato>
   ```

   Si el mandato se ejecuta, entonces es que existe un entorno de shell.

   b. Especifique el nombre entre comillas para que el intérprete de mandatos no lo analice. Por ejemplo, `this is a test.bat argument` se convierte en:

   ```
   "this is a test.bat" argument
   ```

   c. Se pueden utilizar variables de entorno y variables de configuración en el script proporcionado por el usuario, pero no pueden formar parte de la línea de mandatos que inicia el script. Las siguientes variables son excepciones a esta regla:

   AGENT_BIN_DIR
   El directorio en el que el agente coloca los archivos binarios o scripts

   AGENT_ETC_DIR
   El directorio donde el agente coloca los archivos de configuración

   AGENT_LIB_DIR
   El directorio donde el agente coloca las bibliotecas compartidas o las bibliotecas de enlace dinámico

   CANDLEHOME
   El directorio de instalación de Tivoli Monitoring en Linux o UNIX

   CANDLE_HOME
   El directorio de instalación de Windows Tivoli Monitoring

   d. Si se utiliza la opción de recopilación de datos SSH, la línea de mandatos se ejecuta en relación al directorio de inicio del usuario en el sistema remoto. Si carga scripts o ejecutables en el sistema remoto, se copian en la ubicación especificada en la variable de entorno del agente *CDP_SSH_TEMP_DIRECTORY*. La ubicación es, de forma predeterminada, el directorio de inicio del usuario en el sistema remoto. En algunos sistemas, es posible que tenga que definir la línea de mandatos con una vía de acceso relativa, por ejemplo, `./Script.sh`.

6. En el área **Sistemas operativos**, seleccione uno o varios sistemas operativos. Al recopilar datos de un sistema remoto utilizando SSH, Sistemas operativos es una propiedad del sistema en el que el agente está instalado. No es el sistema operativo del sistema remoto. Se recomienda seleccionar el recuadro de selección **Todos los sistemas operativos** cuando se utilizan las características de recopilación de datos SSH.
7. Opcional: Si se necesita uno o varios archivos definidos por el usuario para ejecutar el mandato, pulse **Añadir** en el área de archivos de mandatos para especificar los archivos de su sistema.

   Los archivos se copian en la carpeta del proyecto del agente en `scripts/`*`sistema operativo`*, donde *sistema operativo* es una variable que depende de lo que haya seleccionado en la ventana **Información de mandato**. Estos archivos también se empaquetan y se distribuyen con el agente. Si desea editar la definición de un archivo de mandatos que ya ha añadido, o del que ha cambiado el contenido, seleccione el archivo y pulse **Editar**. Consulte "Edición de una definición de archivo de mandatos" en la página 1318.
8. Pulse **Aceptar**. Se visualiza la página **Lista de mandatos**.
9. Para probar el mandato, utilice los pasos siguientes:
   a) Pulse **Probar** para abrir la información del mandato y visualizar la ventana **Probar mandato**. Para probar el script en un sistema remoto, seleccione un sistema en la lista **Nombre de conexión** o pulse **Añadir** para añadir el nombre de host de un sistema.

   b) Utilice la ventana **Probar mandato** para cambiar el mandato, el separador predeterminado y los separadores de atributos, así como para ver cómo estos cambios afectan a los datos que se devuelven.

      1) Escriba el mandato y el separador en los campos si todavía no están especificados.

         Nota: Puede especificar otros separadores utilizando la ventana **Información de atributos** en el momento de creación de atributos o mediante Agent Editor para modificar un atributo existente. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208 y más información sobre la manipulación de orígenes de datos y atributos, consulte "Edición del origen de datos y propiedades de atributos" en la página 1228
      2) Antes de empezar la prueba, puede establecer variables de entorno y propiedades de configuración. Para obtener más información, consulte ("Prueba de grupo de atributos" en la página 1417).
      3) Pulse **Aceptar** para volver a la ventana **Probar valores**.
      4) Pulse **Iniciar agente**. Una ventana indica que el agente se está iniciando.
      5) Para simular una solicitud de Tivoli Enterprise Portal o SOAP para los datos de agente, pulse **Recopilar datos**. Agent Builder ejecuta su mandato. Si ha especificado un sistema remoto, proporcione un ID de usuario y contraseña. Incluso si el código de retorno no es 0, Agent Builder analiza los resultados del mandato del mismo modo que el agente.
      6) La ventana **Valores de prueba** recopila y muestra los datos de la memoria caché del agente desde que se inició por última vez. Los nombres iniciales de los atributos son **Atributo_1, Atributo_2**, etcétera; sin embargo, puede modificar las propiedades de los atributos pulsando la cabecera de columna apropiada.
      7) Pulse **Comprobar resultados** para ver el código de retorno del mandato, los datos sin analizar y los mensajes de error que se han devuelto.
      8) El agente se puede detener pulsando **Detener agente**.
      9) Pulse **Aceptar** para volver a la ventana **Información de mandato**.

         Si cambia el mandato o el separador, el mandato apropiado se actualiza para reflejar estos cambios.

         Si esta ventana se ha abierto al crear el origen de datos de script, los atributos se han añadido al nuevo origen de datos de script.

Si esta ventana se ha abierto desde un origen de datos de script existente, los cambios en los atributos se realizan en el origen de datos de script. Se añaden los atributos adicionales, pero los atributos de sobra no se eliminan. Estas opciones solo afectan a los atributos analizados desde la salida de script. Los atributos derivados no se ven afectados. Si alguno de estos atributos deja de ser válido basándose en los atributos a los que hacen referencia, puede actualizar o eliminar los atributos derivados manualmente. Se visualiza la fórmula del atributo derivado y no el valor del resultado actual.

Nota: Si el grupo de atributos ya existe, para iniciar una prueba, complete el siguiente procedimiento

a. Seleccione el grupo de atributos en la página **Definición de orígenes de datos** de **Agent Editor**.
b. Seleccione el script que desea probar de la lista de mandatos
c. Pulse **Probar** y siga el procedimiento del paso "9" en la página 1323

10. Si se ha saltado la prueba del mandato en el paso "9" en la página 1323, siga estos pasos:
    a) En la página **Lista de mandatos** con la información de mandatos completada, pulse **Siguiente**.
    b) En la página **Información de atributo**, complete el nombre de atributo y la información del tipo utilizando (Tabla 261 en la página 1234). Seleccione **Añadir atributos adicionales** para añadir más atributos
    c) En la página **Información de atributo**, utilice el separador **Información de atributos de script** para elegir un separador de datos específico para este atributo.

    El separador estándar `;` está seleccionado de forma predeterminada. Puede elegir un número de otros separadores como, por ejemplo, una cadena, un número de caracteres, un separador o un espacio. También puede elegir la utilización de un separador de cadena diferente para el comienzo y finalización de los datos. Finalmente, también puede elegir **Resto del registro** para asignar el resto del registro al atributo. Para obtener más información sobre el análisis de script y los separadores, consulte "Separadores y análisis de script" en la página 1320.
11. Realice una de las acciones siguientes:
    - Si utiliza el **Asistente de agente**, pulse **Siguiente**.
    - Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.
12. Es posible añadir atributos y proporcionar la información para los mismos. Para obtener más información, consulte el apartado "Creación de atributos" en la página 1230.

    Además de los campos aplicables en todos los orígenes de datos (tal como se describe en "Campos y opciones para definir atributos" en la página 1233), la página **Definición de orígenes de datos** para el origen de datos de script tiene las siguientes opciones:

    Lista de mandatos
    Proporciona acceso a los mandatos y scripts para iniciarlos durante la recopilación de datos.

    Añadir
    Permite al usuario añadir un mandato que este grupo de atributos debe iniciar.

    Editar
    Permite al usuario editar una entrada de mandato existente.

    Eliminar
    Permite al usuario suprimir una entrada de mandato existente.

    Probar
    Permite al usuario acceder al entorno de prueba de este grupo de atributos.

    Habilitar la recopilación de datos utilizando SSH
    Al marcar este recuadro de selección se habilita SSH para este grupo de atributos. Si este recuadro de selección no está seleccionado, el grupo de atributos se ejecuta de forma local.

    Si desea más información sobre la configuración de la conexión remota SSH para orígenes de datos de script, consulte "Configuración de una conexión remota de Secure Shell (SSH)" en la página 1407.

Supervisión de datos procedentes de JDBC (Java Database Connectivity)

Puede definir un origen de datos para recibir datos de una base de datos JDBC. El agente ejecuta una consulta SQL para recopilar datos de la base de datos. Cada columna devuelta por la consulta es un atributo en el conjunto de datos resultante.

Acerca de esta tarea

El proveedor de datos JDBC da soporte a los siguientes servidores de bases de datos:

- IBM DB2 9.x y 8.x
- Microsoft SQL Server 2008, 2005 y 2000
- Base de datos Oracle 11g y 10g

Agent Builder no incluye los controladores JDBC correspondientes a estas bases de datos. Los controladores JDBC son un conjunto de archivos JAR proporcionados por el proveedor que son necesarios para establecer una conexión JDBC con la base de datos. Para su comodidad, a continuación se muestran enlaces a los sitios desde los que se pueden descargar estos controladores:

- IBM DB2: los controladores JDBC se incluyen con la instalación del servidor de bases de datos en un subdirectorio llamado `java` situado bajo el directorio principal de instalación de DB2.
- Sitio web de Microsoft SQL Server en www.microsoft.com
- Base de datos Oracle: JDBD de base de datos de Oracle (http://www.oracle.com/technetwork/database/features/jdbc/index.html)

Nota: Es importante recordar que el proveedor de datos JDBC puede supervisar de forma remota los servidores de la base de datos. Un entorno de tiempo de ejecución Java y los archivos JAR del controlador JDBC para el servidor de bases de datos al que se conecta deben estar en el sistema en el que se ejecuta el agente.

Las siguientes versiones de Java están soportadas:

- Oracle Corporation Java Versión 5 o posterior
- IBM Corporation Java Versión 5 o posterior

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos de un servidor** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse en **JDBC**.
3. Pulse **Siguiente**.
4. En el área **Información de JDBC** en la página **Información de JDBC**, pulse **Examinar** para conectarse a una base de datos y crear su consulta SQL.

   Utilice el navegador JDBC para conectarse a una base de datos y ver sus tablas para poder construir una consulta SQL que recopila los datos que necesita. Al seleccionar una tabla y columnas, se genera una consulta para usted y los atributos se añaden para cada una de las columnas devueltas por la consulta. Puede modificar y probar la consulta generada para asegurarse de que los datos que devuelve son los que necesita.

   Nota: También puede crear manualmente el origen de datos JDBC sin pulsar **Examinar**. Si desea crear el origen de datos manualmente, especifique la consulta y pulse **Siguiente**. Debe definir un atributo para cada columna devuelta por la consulta, en el orden en el que se han devuelto las columnas.

   Con el proveedor de datos JDBC, puede ejecutar las consultas SQL y los procedimientos almacenados en una base de datos para recopilar datos de supervisión. Cuando especifique una consulta SQL para recopilar datos, puede incluir una cláusula where en la sentencia SQL para filtrar los datos devueltos. La sentencia SQL también puede unir datos procedentes de diversas tablas. Además de sentencias select de SQL, el proveedor de datos JDBC puede ejecutar procedimientos

almacenados. Para obtener información sobre cómo ejecutar procedimientos almacenados, consulte el apartado "Procedimientos almacenados" en la página 1330.

5. La primera vez que se abre el navegador, la ventana del navegador Java Database Connectivity (JDBC) indica que no se ha seleccionado ninguna conexión. Debe añadir una conexión. Pulse **Añadir** y siga los Pasos para añadir una conexión.

   Si ya ha definido una conexión, se utiliza esa conexión y puede continuar con el paso "6" en la página 1326.

   Nota: El campo **Estatus** muestra el estatus de la conexión actual.

   Siga estos pasos para añadir una conexión:

   a) En la página **Conexiones JDBC**, pulse **Conexión JDBC** y pulse **Siguiente**.

   b) En la página **Propiedades de conexión**, complete los campos del modo siguiente:

      Nombre de conexión
      Nombre de la conexión JDBC. Escriba un nombre exclusivo para esta conexión. Este nombre se utiliza para hacer referencia a la conexión en el navegador.

      Tipo de base de datos
      Tipo de base de datos. Seleccione el producto de base de datos con el que va a establecer conexión. Por ejemplo, para conectar con una base de datos IBM DB2, seleccione **DB2**.

      Nombre de usuario
      Se debe definir por lo menos con acceso de lectura sobre la base de datos, per no es necesario que sea el administrador de bases de datos

      Contraseña
      Se debe definir por lo menos con acceso de lectura sobre la base de datos, pero no es necesario que sea el administrador de bases de datos

      Nombre de host
      Nombre de host en el que se ejecuta el servidor de bases de datos. Con JDBC, puede supervisar bases de datos remotas por lo que no está restringido a supervisar bases de datos del sistema local.

      Puerto
      Puerto del nombre de host en el que escucha el servidor de bases de datos.

      Base de datos
      Nombre de la base de datos con la que se va a establecer conexión.

      Directorio Jar
      Directorio que contiene los archivos JAR de JDBC utilizados para conectar a la base de datos. Escriba el nombre de la vía de acceso o pulse **Examinar** para localizar el directorio.

   c) Opcional: Marque el recuadro de selección **Guardar la contraseña en el espacio de trabajo de Agent Builder** si desea guardar la contraseña para esta conexión.

   d) Opcional: Marque el recuadro de selección **Establecer como valores predeterminados de configuración del agente** si desea que los valores predeterminados para este tipo de servidor de aplicaciones se copien de estas propiedades.

      Si está construyendo el agente en un sistema que es similar a los sistemas supervisados, es aconsejable marcar este recuadro. Si no marca este recuadro, el usuario que configura el agente ve un campo vacío. El usuario entonces deberá determinar los valores para toda la información sin valores predeterminados.

   e) Pulse **Probar conexión** para crear una conexión a la base de datos que utilice los parámetros de configuración que especificó.

      Un mensaje en la página **Propiedades de conexión** indica si la conexión se establece correctamente.

   f) Cuando tenga una conexión en funcionamiento, pulse **Finalizar**.

6. En la ventana **Navegador de JDBC (Java Database Connectivity)**, se realiza una conexión con la base de datos configurada. Las tablas contenidas en la base de datos se muestran en el área **Tablas**

de base de datos. Seleccione una tabla de base de datos para ver las columnas contenidas en esa tabla en el área **Columnas de la tabla seleccionada**.

Nota:

a. Pulse el icono de binoculares para buscar la tabla en la lista **Tablas de la base de datos**.

b. De forma predeterminada se muestran todas las tablas. Puede filtrar las tablas mostradas seleccionando una opción de filtro diferente. Las opciones de filtro disponibles se muestran en la Tabla 267 en la página 1327.

Tabla 267. Opciones de filtro

Opción de filtro	Descripción
Todos	Mostrar todas las tablas
Usuario	Mostrar solo las tablas del usuario
Sistema	Mostrar solo las tablas del sistema
Ver	Mostrar solo las vistas de base de datos

Nota: Si desea recuperar columnas específicas, seleccione solo estas columnas. Si selecciona la tabla, el Agent Builder crea automáticamente una consulta que recopila todas las columnas de la tabla y crea atributos para todas las columnas que están actualmente en la tabla.

Puede seleccionar columnas de las siguientes formas:

- Seleccione la tabla y obtenga la consulta predeterminada para todas las columnas.
- Seleccione columnas para obtener únicamente dichas columnas.

7. Opcional: modifique los valores de enumeración establecidos para Error, Datos faltantes y Ningún valor en la página **Información de atributo**.

   Modifique los valores para evitar cualquier solapamiento con valores legítimos que se pueden devolver de columnas de tabla de base de datos.

8. Opcional: Pulse **Probar** en la ventana **Navegador de Java Database Connectivity (JDBC)** para probar y modificar la sentencia SQL.

   Se abre la ventana **Ejecutar la sentencia SQL**.

   a) Especifique o modifique la sentencia SQL en el campo **Sentencia SQL**.

   b) Pulse **Ejecutar** para ejecutar la sentencia SQL.

   Los resultados se visualizan en el área de **Resultados**. Continúe modificando y probando la sentencia hasta que esté satisfecho con los datos devueltos.

   c) Pulse **Aceptar** para guardar la sentencia, crear los atributos correctos y volver a la ventana **Información de JDBC**.

9. Opcional: Pulse **Probar** en la ventana **Información de JDBC** para probar el grupo de atributos en un entorno de agente más realista. Si desea más información sobre cómo probar grupos de atributos JDBC, consulte “Prueba de grupos de atributos JDBC” en la página 1332. Si cambia la sentencia JDBC durante esta prueba, también debe ajustar los atributos, de forma que hay un atributo por columna devuelta por la sentencia JDBC, en el orden correcto.

10. Opcional: Puede crear un filtro para limitar los datos devueltos por este grupo de atributos al pulsar **Avanzado**. Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte “Filtrado de grupo de atributos” en la página 1239

11. En la página **Información de JDBC**, la sección **Sistemas operativos**, seleccione los sistemas operativos y pulse **Siguiente**. Consulte “Especificación de sistemas operativos” en la página 1251 para obtener información sobre qué sistemas operativos se pueden seleccionar.

    Nota: Pulse **Insertar propiedad de configuración** para seleccionar una propiedad que desee insertar. Para obtener más información, consulte (“Personalización de la configuración del agente” en la página 1401).

12. En la página **Seleccionar atributos clave**, seleccione los atributos clave o indique que este origen de datos solo produce una fila de datos. Para obtener más información, consulte "Selección de atributos clave" en la página 1208.
13. Si desea probar un origen de datos definido previamente, en la ventana Agent Editor, seleccione la pestaña **Orígenes de datos** y seleccione un origen de datos JDBC. En el área **Información de grupo de atributos JDBC**, pulse **Probar**. Para obtener más información sobre la prueba, consulte "Prueba de grupos de atributos JDBC" en la página 1332.
14. Si desea ver las secciones de configuración que se han generado automáticamente, pulse la pestaña **Insertar propiedad de configuración** del Agent Editor.

    Puede cambiar las etiquetas o los valores predeterminados para estas propiedades para que coincidan con los valores predeterminados que el usuario ve al configurar inicialmente al agente.
15. Opcional: Complete la página **Información de atributo**; si desea más detalles, consulte "Campos y opciones para definir atributos" en la página 1233. Realice este paso si elige crear manualmente la fuente de datos JDBC sin pulsar Examinar en el paso "4" en la página 1325.

    El origen de datos JDBC de Agent Builder soporta la recopilación de datos de la mayoría de tipos SQL. La información de Tabla 268 en la página 1328 describe el tipo de atributo que se crea mediante el navegador JDBC cuando detecta una columna de uno de estos tipos. Estos tipos de datos son los tipos de datos soportados para utilizarlos con un agente de supervisión.

Tabla 268. Tipos de datos SQL soportados que se pueden utilizar con un agente de supervisión

Tipo de datos SQL	**Atributo de IBM Tivoli Monitoring que se crea**
BIGINT	Este tipo de datos es un valor de medidor de 64 bits en IBM Tivoli Monitoring. Si selecciona la compatibilidad de IBM Tivoli Monitoring V6.2, es un indicador de 32 bits.
DECIMALDOUBLEFLOATNUMERICREAL	Estos tipos de SQL se crean como atributos de medidos de 64 bits en IBM Tivoli Monitoring. Si los metadatos de base de datos contienen un valor de escala, se utiliza el valor; de lo contrario, la escala se establece en 1. Si selecciona la compatibilidad de IBM Tivoli Monitoring V6.2, el atributo es un indicador de 32 bits.
BITINTEGERSMALLINTTINYINT	Los siguientes tipos de SQL se crean como atributos de medidor de 32 bits en IBM Tivoli Monitoring.
BOOLEAN	Este valor es un indicador de 32 bits en IBM Tivoli Monitoring con enumeraciones para TRUE y FALSE.
TIMESTAMP	Los datos de las columnas de este tipo se convierten en un atributo de indicación de fecha y hora de IBM Tivoli Monitoring de 16 bytes.
TIMEDATECHARLONGVARCHARVARCHAR	El navegador trata todos estos tipos de SQL como atributos de serie. El tamaño de columna se utiliza como tamaño del atributo hasta un máximo de 256, que es el tamaño predeterminado de atributo de serie para el navegador JDBC.

Nota: Si recopila datos de un tipo de datos que no aparece listado, se utiliza de forma predeterminada el atributo de serie. El agente también intenta recopilar los datos de la base de datos como una serie.

modifique los valores de enumeración establecidos para Error, Datos faltantes y Ningún valor en la página **Información de atributo** si es necesario. Modifique los valores para evitar cualquier solapamiento con valores legítimos que se pueden devolver de columnas de tabla de base de datos.

Configuración de JDBC
Cuando se define un origen de datos JDBC en el agente, algunas propiedades de configuración se crean automáticamente.

Si define un origen de datos JDBC en el agente, este debe utilizar Java para conectar con el servidor de bases de datos JDBC. Las propiedades de configuración de Java se añaden al agente automáticamente. Las siguientes propiedades de configuración de Java son específicas de la configuración del tiempo de ejecución del agente:

- *Java Home*: vía de acceso completa que apunta al directorio de instalación Java
- *Argumentos de JVM*: utilice este parámetro para especificar una lista opcional de argumentos para la Java Virtual Machine.
- *Nivel de rastreo*: este parámetro define la cantidad de información que se escribe en el archivo de registro de rastreo de Java. De modo predeterminado, sólo se deben grabar datos de errores en el archivo del registro.

Nota: Agent Builder no necesita las propiedades de Java porque utiliza su propia JVM y registro, que se configuran mediante el plugin `JLog`.

Si se define un origen de datos JDBC en el agente, los siguientes campos de configuración comunes necesarios se añaden al agente automáticamente:

- *Tipo de base de datos JDBC*: tipo de base de datos a la que se conecta, IBM DB2, Microsoft SQL Server u Oracle Database Server.
- *Nombre de usuario JDBC*: nombre de usuario que se utiliza para autenticar con el servidor de bases de datos.
- *Contraseña JDBC*: contraseña que se utiliza para la autenticación con el servidor de bases de datos.
- *Vías de acceso base*: Lista de directorios en los que se buscan archivos JAR nombrados en el campo *Vía de acceso de clases*, o directorios nombrados en el campo *Directorios JAR*, que no estén calificados al completo. Los nombres de directorio están separados por un punto y coma `(;)` en Windows, y por un punto y coma `(;)` o dos puntos `(:)` en sistemas UNIX.
- *Vía de acceso de clase*: archivos JAR nombrados explícitamente para que el agente los busque. Cualquier archivo que no esté cualificado completamente se añade a cada una de las vías de acceso base hasta que se encuentra el archivo JAR.
- *Directorios JAR*: lista de directorios en los que se buscan los archivos JAR. Los nombres de directorio están separados por un punto y coma `(;)` en Windows, y por un punto y coma `(;)` o dos puntos `(:)` en sistemas UNIX. No es necesario identificar explícitamente a los archivos JAR en estos directorios; se encuentran porque residen en uno de estos directorios. No se busca en los subdirectorios de estos directorios. Cualquier directorio que no esté calificado al completo se añadirá a cada una de las vías de acceso base hasta que se encuentre el directorio.

La configuración de tiempo de ejecución también requiere que especifique algunos detalles adicionales para conectar con la base de datos. Puede elegir cómo especificar los elementos de configuración restantes: como un URL de JDBC o como propiedades básicas de configuración (valor predeterminado):

- Opción de configuración de URL
  - URL de conexión JDBC: URL de conexión específica de proveedor que proporciona detalles sobre el host en el que la base de datos está ubicada y el número de puerto al que se debe conectar. El formato de URL suele tener el aspecto siguiente:

    ```
    jdbc:identificador://servidor:puerto/basedatos
    ```

    consulte a documentación del proveedor del controlador JDBC para los distintos formatos de URL.
- Opción de propiedades básicas de JDBC (valor predeterminado)

Nombre del servidor JDBC: nombre del host en el que se ejecuta el servidor de bases de datos.
Nombre de base de datos JDBC: nombre de la base de datos en el host en el que se realiza la conexión.
Número de puerto de JDBC: número de puerto en el que escucha el servidor de bases de datos.

Nota: Con el proveedor de datos JDBC, puede supervisar varios tipos de base de datos del mismo agente utilizando subnodos. Para supervisar de esta forma, debe definir cuidadosamente las Alteraciones temporales de configuración de subnodo. Si supervisa varios tipos de bases de datos, es probable que los siguientes valores de configuración sean diferentes:

- Tipo de base de datos de JDBC
- Nombre de usuario de JDBC
- Contraseña de JDBC

Si utiliza la opción de configuración básica, también deberá definir alteraciones temporales para las siguientes propiedades en la página **Alteraciones temporales de configuración de subnodo**:

- Nombre de servidor de JDBC
- Número de puerto de JDBC
- Nombre de base de datos de JDBC

Para definir las alteraciones temporales de configuración para el subnodo, consulte "Utilización de subnodos" en la página 1384 para obtener más detalles sobre al acceso a la página **Alteraciones temporales de configuración de subnodo**. Al configurar el agente en tiempo de ejecución, se deben configurar todas estas propiedades para cada nueva instancia de subnodo creada.

Además de las alteraciones temporales de configuración, el agente también debe apuntar a controladores JDBC para cada tipo de base de datos a la que tiene pensado conectarse desde los subnodos. El parámetro *Directorios JAR* es la manera más conveniente de apuntar a los controladores JDBC. Liste los directorios que contienen los controladores JDBC utilizando un punto y coma para separar cada directorio. Por ejemplo, si se conecta a bases de datos DB2 y Oracle con el agente, debe especificar un valor de *directorios JAR* similar a este ejemplo: `C:\Archivos de programa\IBM\SQLLIB \java;C:\oracle\jdbc`.

Procedimientos almacenados
Ejemplo de SQL y procedimientos almacenados de DB2 que puede utilizar con el proveedor de datos JDBC.

El proveedor de datos JDBC puede procesar los conjuntos de resultados que devuelve un procedimiento almacenado. Se pueden pasar parámetros de entrada de tipo serie o entero al procedimiento almacenado. La sintaxis siguiente ejecuta un procedimiento almacenado:

```
call[:índice] nombreProcedimiento [argumento] ...
```

Donde:

índice
Un entero opcional que especifica qué conjunto de resultados debe utilizar el proveedor de datos. Este parámetro es útil cuando el procedimiento almacenado devuelve varios conjuntos de resultados y desea recopilar solo los valores de uno de los conjuntos de resultados. Si no se especifica un índice, se recopilan y devuelven datos de cada conjunto de resultados.

nombreProcedimiento
El nombre del procedimiento almacenado que debe ejecutar el proveedor de datos JDBC.

argumento
Un argumento de entrada para el procedimiento almacenado. Si hay varios argumentos, deben separarse mediante comas. Si el argumento contiene un carácter de espacio, especifique todo el argumento entre comillas. Si el argumento se puede analizar como un entero, se pasa al procedimiento almacenado como un argumento de entero. Cualquier argumento entre comillas se pasa como un argumento de cadena.

Ejemplos de SQL Server
`call sp_helpdb`

Ejecuta el procedimiento `call sp_helpdb` que no requiere argumentos. Los datos procedentes de todos los conjuntos de resultados devueltos se incluyen en los datos que devuelve el proveedor de datos.

`call:2 sp_helpdb master`

Ejecuta el procedimiento `sp_helpdb` con el argumento maestro. Se trata de un argumento de entrada de serie. Solo los datos procedentes del segundo conjunto de resultados que devuelve el procedimiento almacenado se incluyen en los datos que devuelve el proveedor de datos.

Si no se especifica el índice, se recopilan datos procedentes de todos los conjuntos de resultados. Debe asegurarse de que los datos devueltos en estos casos sean compatibles con los atributos definidos. Agent Builder crea atributos a partir del primer conjunto de resultados devuelto y se espera que cualquier conjunto de resultados adicional sea compatible con el primero.

Procedimiento almacenado de DB2

Aquí se muestra una función de DB2 de muestra escrita en SQL. Esta función demuestra cómo devolver resultados que pueda procesar el proveedor de datos JDBC de Agent Builder:

```
-- Ejecute este script de la siguiente manera:
-- db2 -td# -vf db2sample.sql

-- Procedimiento para demostrar cómo devolver una consulta desde
-- un procedimiento almacenado de DB2, que posteriormente podrá utilizar
-- un proveedor JDBC de Agent Builder. El procedimiento almacenado
-- devuelve las columnas siguientes:
-- Nombre             Descripción                Tipo de datos
-- current_timestamp  Hora actual del sistema    indicación de fecha y hora
-- lock_timeout       Tiempo de espera de bloqueo  escala numérica 0
-- user               El usuario de la sesión    Cadena de 128 caracteres
DROP procedure db2sample#

CREATE PROCEDURE db2sample()
  RESULT SETS 1
  LANGUAGE SQL
BEGIN ATOMIC

  -- Defina la SQL para la consulta
  DECLARE c1 CURSOR WITH HOLD WITH RETURN FOR
  SELECT CURRENT TIMESTAMP as current_timestamp,
CURRENT LOCK TIMEOUT as lock_timeout, CURRENT USER as user
  FROM sysibm.sysdummy1;

  -- Envíe la consulta y devuelva los datos
  OPEN c1;
END#
```

Esta función se puede llamar desde Agent Builder utilizando la misma sintaxis definida para otros procedimientos almacenados. En este caso, se define `call db2sample` como la sentencia JDBC que debe ejecutar este procedimiento almacenado.

Procedimientos almacenados de Oracle

Los procedimientos almacenados de Oracle no devuelven conjuntos de resultados. El usuario debe escribir una función que devuelva un cursor de referencia de Oracle. Aquí se puede ver una función Oracle de muestra escrita en PL/SQL que demuestra como devolver resultados que pueda procesar el proveedor de datos JDBC de Agent Builder:

```
CREATE OR REPLACE FUNCTION ITMTEST
RETURN SYS_REFCURSOR
IS
        v_rc SYS_REFCURSOR;
COMENZAR
  OPEN v_rc FOR SELECT * FROM ALL_CLUSTERS;
  RETURN v_rc;
END;
```

Esta función se puede llamar desde Agent Builder utilizando la misma sintaxis definida para otros procedimientos almacenados. En este caso, se define `call ITMTEST` como la sentencia JDBC que debe ejecutar este procedimiento almacenado. Puesto que la función de Oracle debe devolver una referencia de cursor, las funciones de Oracle solo pueden procesar un conjunto de resultados. Esto significa que la opción index no recibe soporte para Oracle, ya que no hay manera de devolver varios conjuntos de resultados.

Prueba de grupos de atributos JDBC
Puede probar el grupo de atributos JDBC que ha creado, dentro de Agent Builder.

Procedimiento

1. El procedimiento de prueba se puede iniciar de las siguientes formas:
   - Durante la creación del agente, pulse **Probar** en la página **Información de JDBC**.
   - Tras la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** del Agent Editor y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208.

   Tras pulsar **Probar** en uno de los dos pasos anteriores, se visualiza la ventana **Probar sentencia JDBC**.
2. Opcional: Antes de iniciar la prueba, puede establecer variables de entorno, propiedades de configuración e información de Java.

   Para obtener más información, consulte "Prueba de grupo de atributos" en la página 1417. Para obtener más información sobre las propiedades de configuración, consulte "Configuración de JDBC" en la página 1329.
3. Pulse **Iniciar agente**.

   Una ventana indica que el agente se está iniciando.
4. Para simular una solicitud de Tivoli Enterprise Portal o SOAP para los datos de agente, pulse **Recopilar datos**.

   El agente consulta la base de datos con la consulta SQL especificada. La ventana **Probar sentencia JDBC** recopila y muestra los datos en la memoria caché del agente desde la última vez que se inició.

   Nota: El orden de los datos devueltos es significativos; por ejemplo, el valor de los datos en la primera columna devuelta siempre se asigna al primer atributo. Si cambiar la sentencia JDBC, debe añadir, eliminar o reordenar los atributos para comparar las columnas devueltas por la sentencia.
5. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana Estado de recopilación de datos recopila y muestra, se describen en "Nodo Estatus de objeto de rendimiento" en la página 1462
6. Detenga el agente pulsando **Detener agente**.
7. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Probar sentencia JDBC**. Al pulsar **Aceptar** se guardan los cambios realizados.

Conceptos relacionados
"Pruebas del agente en Agent Builder" en la página 1417
Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión de la disponibilidad del sistema mediante ping

Puede definir un origen de datos para probar una lista de dispositivos de red utilizando el ping de eco ICMP (protocolo de mensajes de control de Internet). El nombre de host o la dirección IP de los dispositivos que desea probar se listan en uno o varios archivos de lista de dispositivos. Un archivo de configuración de ping aparte especifica la vía de acceso a cada archivo de lista de dispositivos. A continuación, el nombre del archivo de configuración de ping se establece en la configuración del agente de tiempo de ejecución. Los resultados incluyen el estado de cada dispositivo de red.

Antes de empezar

Cree archivos de lista de dispositivos y un archivo de configuración de ping (consulte "Archivos de configuración" en la página 1333).

Acerca de esta tarea

Parte de la gestión de red implica la posibilidad de determinar si los sistemas responden a un ping del protocolo de mensajes de control de Internet (ICMP). Utilice este origen de datos para supervisar el estado básico en línea o fuera de línea de un conjunto de servidores u otros dispositivos críticos del entorno. La supervisión con ping es simple y conlleva poca sobrecarga. Para supervisar una lista de dispositivos, añada el recopilador de datos Ping al agente.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos de gestión de red** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse en **Ping**.
3. Pulse **Siguiente**.
4. En el área **Sistemas operativos** en la ventana **Información de ping**, seleccione los sistemas operativos.
5. Opcional: Puede probar este grupo de atributos pulsando **Probar**. Para obtener más información sobre pruebas, consulte "Prueba de grupos de atributos de ping" en la página 1334
6. Opcional: Puede crear un filtro para limitar los datos que este grupo de atributos devuelve pulsando **Avanzado**. Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte "Filtrado de grupo de atributos" en la página 1239
7. Realice una de las acciones siguientes:
   a) Si utiliza el **Asistente de agente**, pulse **Siguiente**.
   b) Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.
8. Para obtener más información sobre la adición de atributos, consulte "Creación de atributos" en la página 1230.

Resultados

Si desea más información sobre el grupo de atributos para Ping, consulte "Grupo de atributos de ping" en la página 1492.

Archivos de configuración

Puede utilizar archivos de configuración para proporcionar al agente la lista de dispositivos a los que realizar ping.

El agente necesita dos tipos de archivos de configuración.

Archivo de lista de dispositivos

Incluye una lista de dispositivos a los que realizar ping. Si tiene muchos dispositivos puede dividirlos en varios archivos de lista de dispositivos. El agente inicia una hebra aparte para cada archivo de lista de dispositivos y pasa por los archivos en paralelo. Pasa por cada archivo cada 60 segundos o cada 30 segundos más el tiempo que tarda en realizar ping para la lista, lo que tarde más.

La sintaxis del archivo de lista de dispositivos es la siguiente:

```
LISTNAME=nombre_lista
nombre_dispositivo o nombre_host
nombre_dispositivo o nombre_host
nombre_dispositivo o nombre_host nombre_dispositivo o nombre_host
```

Donde *nombre_lista* es una descripción de los dispositivos de ese archivo. Si no se ha definido ningún nombre de lista, se utilizará el nombre del archivo de lista de dispositivos. No es necesario que el

nombre de lista sea la primera entrada del archivo. Sin embargo, si el archivo tiene varias definiciones de nombre de lista, se utiliza la última definición.

No existe límite al número de dispositivos que puede incluir en un archivo de lista de dispositivos. No obstante, incluir demasiadas entradas frustra el objetivo de tener una lista de destino de dispositivos críticos y aumenta la carga de trabajo global. Puede ser más difícil recuperar el estado de cada dispositivo dentro del intervalo de supervisión de 60 segundos.

Al principio de cada ciclo, el agente comprueba la hora de la última modificación del archivo de lista de dispositivos. Si la hora de la última modificación del archivo es más reciente que la hora de la última vez que el agente ha leído el archivo, el agente vuelve a leer el archivo sin necesidad de un reinicio.

Archivo de configuración de ping
Especifica la ubicación de archivo de lista de dispositivos. Utilice la vía de acceso totalmente calificada o una vía de acceso relativa a la ubicación del archivo de configuración de ping. El archivo de configuración de ping se pasa al agente como parámetro de configuración de tiempo de ejecución.

Ejemplo

En el ejemplo siguiente, los dispositivos se dividen en dos archivos.
El archivo `/data/retailList.txt` contiene las entradas siguientes:

```
LISTNAME=Retail
frontend.mycompany.com
productdb.mycompany.com
```

El archivo `/data/manufacturingList.txt` contiene las entradas siguientes:

```
LISTNAME=Manufacturing systems
manufloor.mycompany.com
stats.supplier.com
```

El archivo de ping, `/data/pinglists.txt`, contiene las entradas siguientes:

```
/data/retailList.txt
/data/manufacturingList.txt
```

Propiedad de configuración de Network Management

Después de añadir un origen de datos de ping, la configuración se visualiza en la página **Información de configuración de tiempo de ejecución** de Agent Editor.

La sección **Gestión de red** de la página **Información de configuración de tiempo de ejecución** contiene la siguiente propiedad:

Tabla 269. Propiedades de configuración de gestión de red

Nombre	Valores válidos	Necesario	Descripción
`Archivo de configuración de ping`	Vía de acceso a un archivo	No. Si este archivo no se proporciona, se utiliza el archivo `KUMSLIST` del directorio bin del agente.	La vía de acceso para el archivo que contiene una lista de archivos, que contienen cada uno una lista de hosts que se deben supervisar mediante pings de ICMP.

Prueba de grupos de atributos de ping
Puede probar el grupo de atributos de ping que ha creado dentro de Agent Builder.

Procedimiento

1. El procedimiento de prueba se puede iniciar de las siguientes formas:

- Durante la creación del agente, pulse **Probar** en la página **Información de ping**.
- Tras la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** del Agent Editor y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208.

Después de pulsar **Probar** en uno de los dos pasos anteriores, se abre la ventana **Probar valores**.

2. Opcional: Antes de empezar la prueba, puede establecer variables de entorno y propiedades de configuración. Para obtener más información, consulte "Prueba de grupo de atributos" en la página 1417.
3. Pulse **Examinar** para seleccionar un archivo de configuración de ping. Para obtener más información sobre los archivos de configuración de ping, consulte "Archivos de configuración" en la página 1333
4. Pulse **Iniciar agente**. Una ventana indica que el agente se está iniciando.
5. Para simular una solicitud desde el entorno de supervisión para los datos de agente, pulse **Recopilar datos**. El agente hace ping a los dispositivos que se especifican en el archivo de lista de dispositivos, al que se hace referencia desde el archivo de configuración de ping.
6. La ventana **Probar valores** recopila y muestra los datos de la memoria caché del agente desde que se inició por última vez.
7. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que se recopilan y muestran mediante la ventana Estado de colección de datos se describen en "Nodo Estatus de objeto de rendimiento" en la página 1462.
8. Detenga el agente pulsando **Detener agente**.
9. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Probar valores**. Al pulsar **Aceptar** se guardan los cambios que ha realizado.

Conceptos relacionados

"Pruebas del agente en Agent Builder" en la página 1417
Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión de la disponibilidad de HTTP y del tiempo de respuesta

Puede configurar un origen de datos para supervisar la disponibilidad y el tiempo de respuesta de los URL seleccionados. Utilice un archivo de configuración para definir una lista de URL. Establezca el nombre del archivo en la configuración de tiempo de ejecución del agente. En IBM Tivoli Monitoring, puede utilizar también los mandatos de actuación para agregar y eliminar los URL supervisados. El estado de cada URL se añade como una línea en el conjunto de datos resultante.

Acerca de esta tarea

Para cada URL que supervisa, los resultados proporcionan información general sobre la respuesta de HTTP a la solicitud de HTTP. Los resultados incluyen si se puede recuperar, cuánto tiempo tarda la recuperación y el tamaño de la respuesta. Si el contenido de la respuesta es HTML, también se proporciona información sobre los objetos de página en el URL.

Puede supervisar los URL que utilicen los protocolos HTTP, HTTPS, FTP y de archivos. Especifique los URL que se vayan a supervisar en el archivo de los URL HTTP o mediante las opciones de Actuación.

Importante: En el momento del release, los mandatos de actuación no están disponibles en un entorno de IBM Cloud Application Performance Management. Solo están disponibles en un entorno de Tivoli Monitoring.

Este origen de datos requiere el entorno de tiempo de ejecución Java. Las siguientes versiones de Java están soportadas:

- Oracle Corporation Java Versión 5 o posterior
- IBM Corporation Java Versión 5 o posterior

Utilice el siguiente procedimiento para crear un grupo de atributos para supervisar una lista de URL:

Procedimiento

1. En las páginas **Origen de datos inicial de agente** o **Ubicación de origen de datos**, pulse **Datos de un servidor** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse en **HTTP**.
3. Pulse **Siguiente**.
4. En la página **Información de HTTP**, seleccione uno o más sistemas operativos en el área **Sistemas operativos**.
5. Opcional: Pulse **Probar** para probar este grupo de atributos. Para obtener más información sobre pruebas, consulte "Prueba de grupos de atributos de HTTP" en la página 1343
6. Opcional: Pulse **Avanzado** para crear un filtro para limitar los datos devueltos por este grupo de atributos. Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte "Filtrado de grupo de atributos" en la página 1239
7. Realice una de las acciones siguientes:
   a) Si utiliza el **Asistente de agente**, pulse **Siguiente**.
   b) Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.

Resultados

El origen de datos de HTTP crea dos grupos de atributos: URL gestionados y objetos URL. Puede añadir, modificar o suprimir atributos.

Tareas relacionadas

"Creación de atributos" en la página 1230
Puede añadir atributos nuevos a un conjunto de datos.

Referencia relacionada

"Grupos de atributos HTTP" en la página 1495
Los dos grupos de atributos HTTP, `URL gestionados` y `Objetos de URL`, se utilizan para recibir información de los URL y los objetos contenidos en estos URL.

Tablas HTTP

Información de referencia acerca de los grupos de atributos de HTTP.

Los dos grupos de atributos creados por el origen de datos HTTP son:

`URL gestionados`
: Las tablas de los URL gestionados proporcionan disponibilidad y datos de tiempo de respuesta sobre cada URL que se está supervisando.

`Objetos de URL`
: La tabla Objetos de URL contiene una entrada de URL distinta para cada objeto incrustado. Por ejemplo, los archivos `.gif` y `.jpg` que se pueden utilizar en el sitio web listado en el informe URL gestionado.

Para obtener información sobre la sintaxis utilizada en las tablas de URL gestionadas y Objetos URL, consulte ("Campos específicos para atributos HTTP" en la página 1337).

Cuando desee supervisar el tiempo de respuesta y la disponibilidad de objetos específicos en un sitio web, revise el contenido de la tabla Objetos URL. La tabla Objetos URL supervisa una lista de objetos específica que se detectan en archivos HTML descargados. La siguiente tabla lista los elementos HTML en los que se buscan objetos para supervisar y los atributos dentro de esos elementos que hacen referencia a los objetos:

Tabla 270. Elementos HTML en los que se buscan objetos para supervisar

Elemento HTML	**Atributo que contiene el objeto que se va a supervisar**
`img`	`src`
`script`	`src`

Tabla 270. Elementos HTML en los que se buscan objetos para supervisar (continuación)	
Elemento HTML	**Atributo que contiene el objeto que se va a supervisar**
incorporar	src
objeto	codebase o datos
cuerpo	segundo plano
entrada	src

En el siguiente ejemplo de extracto de HTML, el objeto supervisado es la imagen a la que hace referencia el atributo src del elemento img.

```
<img src="/v8/images/id-w3-sitemark-simple.gif" alt="" width="54" height="33" />
```

El URL completo para la imagen se calcula en base al URL para el documento de origen.

Nota: Si no desea supervisar objetos que se encuentren en una página web, en la sección de configuración de la supervisión de URL, establezca la propiedad **Recopilación de objetos de página** en **No**.

Campos específicos para atributos HTTP

En la página **Información de atributos**, hay dos campos para los atributos HTTP que definen cómo se recopilan los datos desde el URL. El campo **Tipo de atributo** puede ser cualquier valor de una lista que controle la información sobre el URL que se ha devuelto. Algunos tipos de atributos requieren un valor en el campo **Valor de tipo**.

La siguiente tabla describe todos los tipos de atributos para el grupo de atributos de URL gestionados y el valor de tipo cuando uno es necesario:

Tabla 271. Información de atributos HTTP - URL gestionados				
Tipo de atributo	**Descripción**	**Valor de tipo**	**Tipo de datos devueltos**	**Diferencias con los protocolos FTP y de archivos**
XPath Query	Ejecuta una consulta XPath en el contenido devuelto desde una conexión URL. La consulta se debe grabar para que devuelva datos útiles para un atributo, no una lista de nodos.	La consulta XPath que se ejecutará en el contenido que se obtiene de una conexión URL.	Los datos devueltos pueden ser un valor de serie, un valor numérico o un valor de indicación de fecha y hora. Si los datos están el formato DateTime de XML, puede especificar la indicación de fecha y hora como tipo de atributo. El agente convierte el valor a Timestamp de Candle.	Ninguna

Tabla 271. Información de atributos HTTP - URL gestionados (continuación)

Tipo de atributo	Descripción	Valor de tipo	Tipo de datos devueltos	Diferencias con los protocolos FTP y de archivos
`Tiempo de respuesta`	La cantidad de tiempo en milisegundos que se ha tardado en descargar el contenido del URL solicitado.	Ninguno	Entero (número de milisegundos)	Ninguna
`Mensaje de respuesta`	El mensaje de respuesta de HTTP que devuelve el servidor.	Ninguno	Serie	El mensaje de respuesta se aplica solo si el URL utiliza protocolos HTTP o HTTPS.
`Código de respuesta`	El código de respuesta de HTTP que devuelve el servidor.	Ninguno	Entero	El código de respuesta se aplica solo si el URL utiliza protocolos HTTP o HTTPS. Siempre es 0 para los URL de archivos o de FTP.
`Longitud de respuesta`	El tamaño del contenido en bytes que se descarga desde el URL solicitado	Ninguno	Entero (tamaño en bytes)	Ninguna
`Cabecera de respuesta`	La cabecera de respuesta se puede utilizar para recuperar un valor de uno de los campos de cabecera de respuesta de URL. El argumento especifica qué campo es solicitado.	La cabecera de respuesta a recopilar.	Serie	Normalmente los protocolos de archivo y FTP no tienen cabeceras que se puedan recopilar.

Tabla 271. Información de atributos HTTP - URL gestionados (continuación)

Tipo de atributo	Descripción	Valor de tipo	Tipo de datos devueltos	Diferencias con los protocolos FTP y de archivos
`Solicitar URL`	La conexión se realiza para este URL. Todas las palabras claves de respuesta proporcionan información sobre la conexión con este URL. La consulta XPath se puede utilizar para obtener información que se consigue del contenido que se ha devuelto accediendo a este URL.	Ninguno	Serie	Ninguna
`Objetos de página`	Número de objetos descubiertos en la página HTML supervisada que son supervisados por el grupo de atributos Objetos URL.	Ninguno	Entero	Ninguna
`Tamaño total de objeto`	Tamaño total del objeto supervisado en el grupo de atributos Objetos URL para esta página web.	Ninguno	Entero (en bytes)	Ninguna
`Alias`	Alias especificado por el usuario para este URL.	Ninguno	Serie	Ninguna
`Usuario`	Datos especificados por el usuario para este URL.	Ninguno	Serie	Ninguna

La siguiente tabla describe los tipos de atributo para el grupo de atributos Objetos URL:

Tabla 272. Información de atributos HTTP - Objetos de URL				
Tipo de atributo	**Descripción**	**Valor de tipo**	**Tipo de datos devueltos**	**Diferencias con los protocolos FTP y de archivos**
URL	El URL que se supervisa en la tabla URL gestionados.	Ninguno	Serie	Ninguna
`Nombre de objeto`	El URL para el objeto que se supervisa en la página **HTML**.	Ninguno	Serie	Ninguna
`Tamaño de objeto`	El tamaño en bytes del contenido descargado desde el URL de Nombre de objeto.	Ninguno	Numérico	Ninguna
`Tiempo de respuesta de objeto`	El tiempo en milisegundos que tarda en descargarse el objeto de página.	Ninguno	Numérico	Ninguna

Supervisión de un URL

Puede empezar a supervisar cualquier URL inclúyendolo en el archivo de los URL o utilizando la opción de actuación Añadir URL HTTP.

Archivo de URL

El archivo de URL especificado en la configuración puede estar en cualquier directorio. Si este archivo no existe o está vacío, podrá iniciar la supervisión de URL utilizando Actuaciones. Para obtener más información, consulte “Opción de Actuación” en la página 1341. Si ya tiene Tivoli Universal Agent que utiliza el Proveedor de datos HTTP de Tivoli Universal Agent, podrá reutilizar el archivo KUMPURLS. Cuando configura el agente, apunte al archivo KUMPURLS.

La tabla siguiente proporciona ejemplos de cómo se entran los URL en el archivo de URL, en función del método por el que se añaden.

Tabla 273. Entradas de archivo de URL	
URL	**Añadido por**

`www.bbc.co.uk`
`http://weather.com`
`www.ibm.com`
	Adición de entradas de forma manual al archivo. Si no se especifica ningún protocolo, como en el ejemplo de `www.ibm.com`, se adopta el http.

`ftp://userid:password@ftpserver/index.html`	Añadido manualmente mediante el protocolo de transferencia de archivos (FTP)
`http://www.ibm.com USER=ibm ALIAS=ibm`	Utilización de la actuación Añadir URL HTTP
`file:/tmp/samples.html USER=samples \` `ALIAS=samples`	Utilización de una actuación Añadir URL HTTP que utiliza FTP

Tabla 273. Entradas de archivo de URL (continuación)	
URL	**Añadido por**
`http://google.com INTERVAL=60 CACHE=50 \ USER=google ALIAS=search`	Ejemplo del archivo KUMPURLS de Tivoli Universal Agent

Cuando edita el archivo de URL directamente, los cambios se implementan cuando el agente realiza la siguiente recopilación de datos.

Opción de Actuación

También puede especificar los URL para supervisar a través de una opción de actuación que se llama `Añadir URL HTTP`.

Restricción: Esta opción no está disponible en el release actual de IBM Cloud Application Performance Management, porque no puede iniciar los mandatos de actuación manualmente.

Cuando se selecciona esta opción, aparecerá una ventana donde puede especificar los siguientes parámetros:

URL
: Un parámetro necesario que representa al propio URL. Puede escribir este parámetro con o sin los prefijos `http://`o `https://`.

Alias
: Un parámetro opcional que puede especificar para asociar un nombre más significativo a un URL. No se permiten espacios en este parámetro. Si este parámetro no está completo, el nombre de alias se establece de forma predeterminada en blanco.

User_Data
: Un parámetro opcional que puede especificar para entrar datos sobre el URL. Si este parámetro no está completo, `User_Data` es `INITCNFG` de forma predeterminada.

Después de completar la información y cerrar la ventana, asigne la acción `HTTP URL Add` al sistema gestionado de destino asociado con el agente. La supervisión se inicia inmediatamente para el nuevo URL. El URL también se añade al archivo de URL por lo que se sigue supervisando durante los reinicios del agente.

Una opción de actuación correspondiente se denomina `Eliminación de URL HTTP`. Utilice la acción `Eliminación de URL HTTP` para detener inmediatamente la supervisión para un URL en particular. El URL eliminado también es suprimido del archivo de los URL. La ventana **Eliminar URL HTTP** solicita solo los valores de URL y `User_Data`. Los valores URL y `User_Data` deben coincidir los valores que aparecen en el Tivoli Enterprise Portal o la acción Eliminar fallará. Por ejemplo, si omitió `http://` en el campo URL de la acción Añadir, debe incluirlo en el campo URL de la acción Eliminar. Si no especificó `User_Data`, debe especificar `INITCNFG` como aparece en el Tivoli Enterprise Portal.

Si un URL se añade manualmente al archivo de URL, puede suprimirlo con la Actuación. Si suprime con la acción Actuación, debe especificar los valores como aparecen en el Tivoli Enterprise Portal. Por ejemplo, si añadió `www.ibm.com` al archivo de URL, el Tivoli Enterprise Portal muestra `http://www.ibm.com` como el URL y `INITCNFG` como `User_Data`. Para eliminar el URL con la Actuación, debe utilizar los valores que aparecen en el Tivoli Enterprise Portal.

Tras completar la información y cerrar la ventana, asigne la acción `Eliminar URL HTTP` al sistema gestionado de destino que está asociado al agente.

Supervisor de los URL `https://`

El origen de datos de HTTP solo puede supervisar los URL `https://` seguros que no requieren el acceso mediante script ni solicitudes interactivas.

Si el URL `https://` se puede recuperar con una llamada Get de HTTP estándar, se puede supervisar.

Servidor proxy
Si el sistema en el que se está ejecutando el agente requiere un proxy para acceder al proveedor de datos SOAP, debe especificar las propiedades de configuración del servidor proxy.

Para obtener más información, consulte el apartado "Configuración del servidor proxy" en la página 1342.

Configuración de HTTP
Información de referencia sobre la configuración de HTTP.

Después de añadir un origen de datos HTTP, la configuración se visualiza en la página **Configuración de tiempo de ejecución** de Agent Editor. Se añaden las secciones de configuración para supervisión de URL, para la autenticación del servidor Proxy y para Java.

Configuración de la supervisión de URL

La sección Configuración de supervisión de URL contiene las siguientes propiedades:

Tabla 274. Propiedades de configuración de supervisión de URL

Nombre	Valores válidos	Necesario	Descripción
Archivo de los URL HTTP	Vía de acceso a un archivo	Sí	La vía de acceso para el archivo que contiene una lista de URL.
Recopilación de objetos de página	Sí, no El valor predeterminado es Sí.	No	Si descargar objetos encontrados en una página web y recopilar los datos de estos objetos.

Configuración del servidor proxy

La sección Configuración del servidor proxy contiene las siguientes propiedades:

Tabla 275. Propiedades de configuración de servidor Proxy

Nombre	Valores válidos	Necesario	Descripción
Nombre de host de proxy	Serie	No	El nombre de host del proxy que se va a utilizar para las conexiones HTTP.
Nombre de usuario de proxy	Serie	No	El nombre de usuario para el servidor proxy.
Puerto del proxy	Entero positivo El valor predeterminado es 80.	No	El número de puerto HTTP del servidor proxy.
Contraseña de proxy	Contraseña	No	La contraseña para el servidor proxy.

Nota: Si la propiedad del **Nombre de host de proxy** está vacío, no se utilizará ningún proxy.

La configuración de Java

Si define un origen de datos HTTP en el agente, este debe utilizar Java para conectarse al servidor HTTP. Las propiedades de configuración de Java se añaden al agente automáticamente. Las siguientes propiedades de configuración de Java son específicas de la configuración del tiempo de ejecución del

agente. Agent Builder no necesita las propiedades de Java porque utiliza su JVM e inicio de sesión propios, que se configuran a través del plug-in JLog:

Tabla 276. Propiedades de configuración de Java

Nombre	Valores válidos	Necesario	Descripción
Directorio inicial de Java	Vía de acceso completa a un directorio	No	Una vía de acceso completa que apunta al directorio de instalación de Java.
Nivel de rastreo	Opción (El valor predeterminado es Error)	Sí	Utilice esta propiedad para especificar el nivel de rastreo utilizado por los proveedores de Java.
Argumentos de JVM	Serie	No	Utilice esta propiedad para especificar una lista opcional de argumentos para la máquina virtual de Java.

Prueba de grupos de atributos de HTTP
Puede probar el grupo de atributos HTTP ha creado, dentro de Agent Builder.

Procedimiento

1. Inicie el procedimiento de prueba de las siguientes formas:
   - Durante la creación del agente, pulse **Probar** en la página **Información de HTTP**.
   - Tras la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** del Agent Editor y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208

   Tras pulsar **Probar** en uno de los dos pasos anteriores, se muestra la ventana **Prueba de HTTP**.
2. Pulse **Examinar** para seleccionar el archivo de URL de HTTP. Si desea más información sobre archivos de URL, consulte "Archivo de URL" en la página 1340.
3. Opcional: Antes de iniciar la prueba, establezca las variables de entorno, las propiedades de configuración y la información de Java.

   Para obtener más información, consulte "Prueba de grupo de atributos" en la página 1417. Si desea más información sobre la configuración de HTTP, consulte "Configuración de HTTP" en la página 1342.
4. Pulse **Iniciar agente**.

   Una ventana indica que el agente se está iniciando.
5. Para simular una solicitud de Tivoli Enterprise Portal o SOAP para los datos de agente, pulse **Recopilar datos**.

   El agente supervisa los URL definidos en el archivo de los URL HTTP. La ventana **Prueba de HTTP** muestra todos los datos que se devuelven.
6. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana Estado de recopilación de datos recopila y muestra, se describen en "Nodo Estatus de objeto de rendimiento" en la página 1462
7. Detenga el agente pulsando **Detener agente**.
8. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Prueba de HTTP**. Al pulsar **Aceptar** se guardan los cambios realizados.

Conceptos relacionados
"Pruebas del agente en Agent Builder" en la página 1417

Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión de datos de un origen de datos SOAP u otro origen de datos HTTP

Puede definir un origen de datos para recibir datos de un servidor HTTP (por ejemplo, mediante el protocolo SOAP). El origen de datos envía una solicitud HTTP a un URL y analiza la respuesta (en formatos XML, HTML o JSON) en los atributos del conjunto de datos resultante. Puede seleccionar los datos recuperados de la solicitud.

Acerca de esta tarea

Mediante la utilización del origen de datos SOAP, puede especificar un URL de HTTP y enviar una solicitud GET, POST o PUT. Para las solicitudes POST o PUT, puede especificar los datos POST asociados. Se recupera y analiza una respuesta XML, HTML o JSON y los datos se exponen en el entorno de supervisión en los atributos. Puede definir los atributos como todos los valores dentro de un elemento en particular. O bien puede definir valores de XPath personalizados para especificar cómo llenar atributos individuales. También puede combinar los dos mecanismos.

Utilice el siguiente procedimiento para recopilar respuestas XML, HTML o JSON de un URL:

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Datos de un servidor** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse en **SOAP**.
3. Pulse **Siguiente**.
4. En la página **Información de SOAP**, especifique un URL.

   El valor predeterminado es:

   ```
   http://${KQZ_HTTP_SERVER_NAME}:${KQZ_HTTP_PORT_NUMBER}
   ```

   Nota: Puede utilizar una variable de configuración o varias variables de configuración que se resuelvan en un URL. Pulse **Insertar propiedad de configuración** para seleccionar una propiedad que desee insertar. Para obtener más información, consulte el apartado “Personalización de la configuración del agente” en la página 1401.
5. Seleccione un tipo de solicitud. El tipo de solicitud predeterminada es Get. Para las solicitudes Post y Put, especifique los datos que se vayan a procesar.

   Nota: Para las solicitudes Post y Put, se habilita **Insertar propiedad de configuración**. Pulse en **Insertar propiedad de configuración** para incluir una variable de configuración en los datos que se van a procesar. Para obtener más información, consulte (“Personalización de la configuración del agente” en la página 1401).
6. Pulse **Examinar**

   Nota: Si después de entrar un URL y seleccionar un tipo de solicitud, no desea utilizar el navegador de SOAP para crear la definición, especifique un **XPath de selección de filas**. El **XPath de selección de filas** en la ventana **Información de SOAP**. A continuación, defina todos los atributos para el grupo de atributos.
7. En la ventana **Navegador de SOAP**, realice los pasos siguientes:
   a) Entre un URL y seleccione un tipo de solicitud si todavía no lo ha hecho.
   b) Pulse **Configuración** para establecer las propiedades de configuración referenciadas en el URL o en otros campos.
   c) Pulse en **Conectar** para obtener datos del proveedor de SOAP.

      Cuando se conecta al URL, una lista de elementos XML para este URL se muestra en un árbol DOM (modelo de objetos de documento). Una respuesta HTML o JSON se convierte en XML y se visualiza como un árbol de DOM. Para conocer detalles sobre la conversión de una respuesta

JSON a XML, consulte “Representación XML de datos JSON” en la página 1347. En el ejemplo de WebSphere Application Server de la Figura 44 en la página 1345, se ha entrado el siguiente URL:

```
http://nc053011.tivlab.raleigh.ibm.com:9080/wasPerfTool/servlet
/perfservlet?module= \threadPoolModule
```

Se muestra el elemento XML `PerformanceMonitor`. Este elemento es el elemento XML de nivel superior del documento XML que devuelve el proveedor de SOAP.

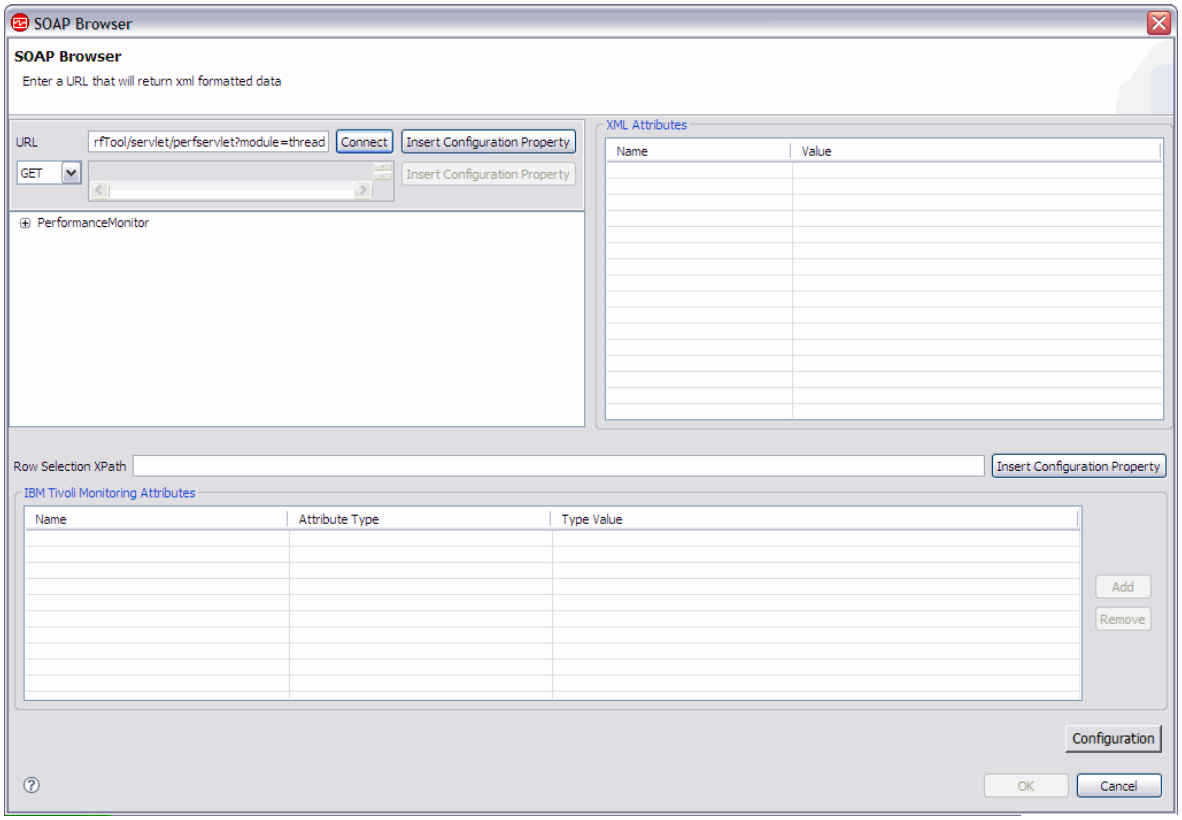


*Figura 44. Ventana **Navegador de SOAP***

d) En el árbol de DOM, busque y seleccione el nodo XML que desea establecer como el **XPath de selección de filas**.

En el ejemplo de WebSphere Application Server de la Figura 45 en la página 1346, el nodo `PerformanceMonitor/Node/Server/Stat/Stat/Stat` está seleccionado. Este nodo representa una fila de datos en el grupo de atributos. Cuando selecciona un nodo en el árbol DOM y pulsa **Añadir**, se obtienen todos los atributos y elementos definidos en ese nodo del árbol. (Puede pulsar **Añadir** en el área **Atributos de agente**).

Cuando se selecciona un nodo, el área **Atributos de XML** muestra los atributos XML definidos para el nodo seleccionado. Seleccione un atributo XML y pulse **Añadir**para incluir este atributo en la lista de atributos del agente.

Nota: Si se espera más de una fila de datos, XPath debe correlacionar una conjunto de nodos. Cuando el XPath de selección de filas devuelve un nodo que está establecido con solo un elemento, el grupo de atributos contiene una única fila.

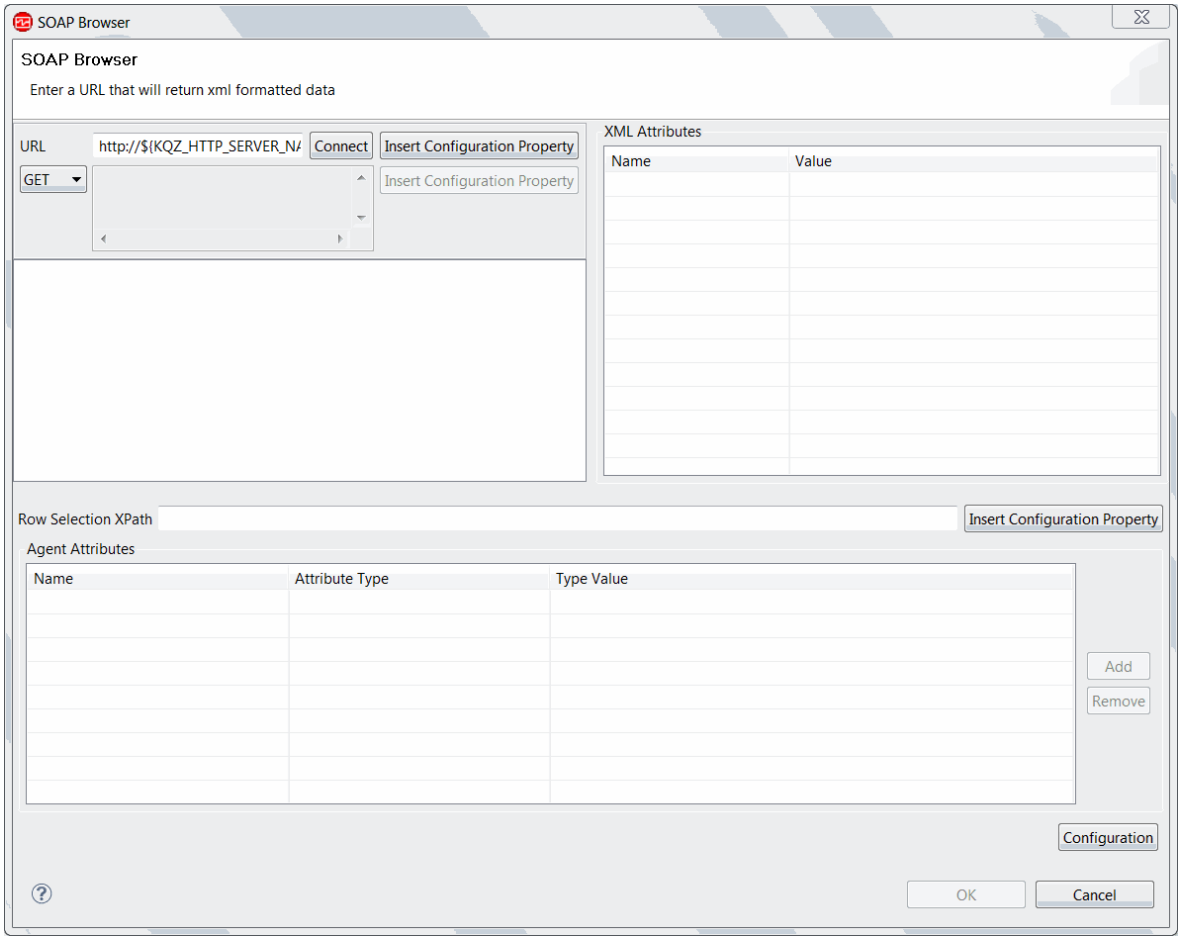


*Figura 45. Ventana **Navegador de SOAP***

e) Pulse **Añadir** en el área Atributos de agente.

Se muestra la lista de atributos de agente y el campo **XPath de selección de filas** se llena.

El XPath para cada atributo de agente se utiliza para correlacionar nodos XML o elementos con atributos de agente. En el ejemplo de WebSphere Application Server en Figura 46 en la página 1347, el primer atributo de la lista de atributos de agente, `Stat`, no se utiliza y se eliminará.

Puede editar el nombre y el XPath para un atributo de agente en el campo **Valor de tipo**. Para obtener más información sobre cómo utilizar XPaths, consulte "Opciones de XPath" en la página 1350

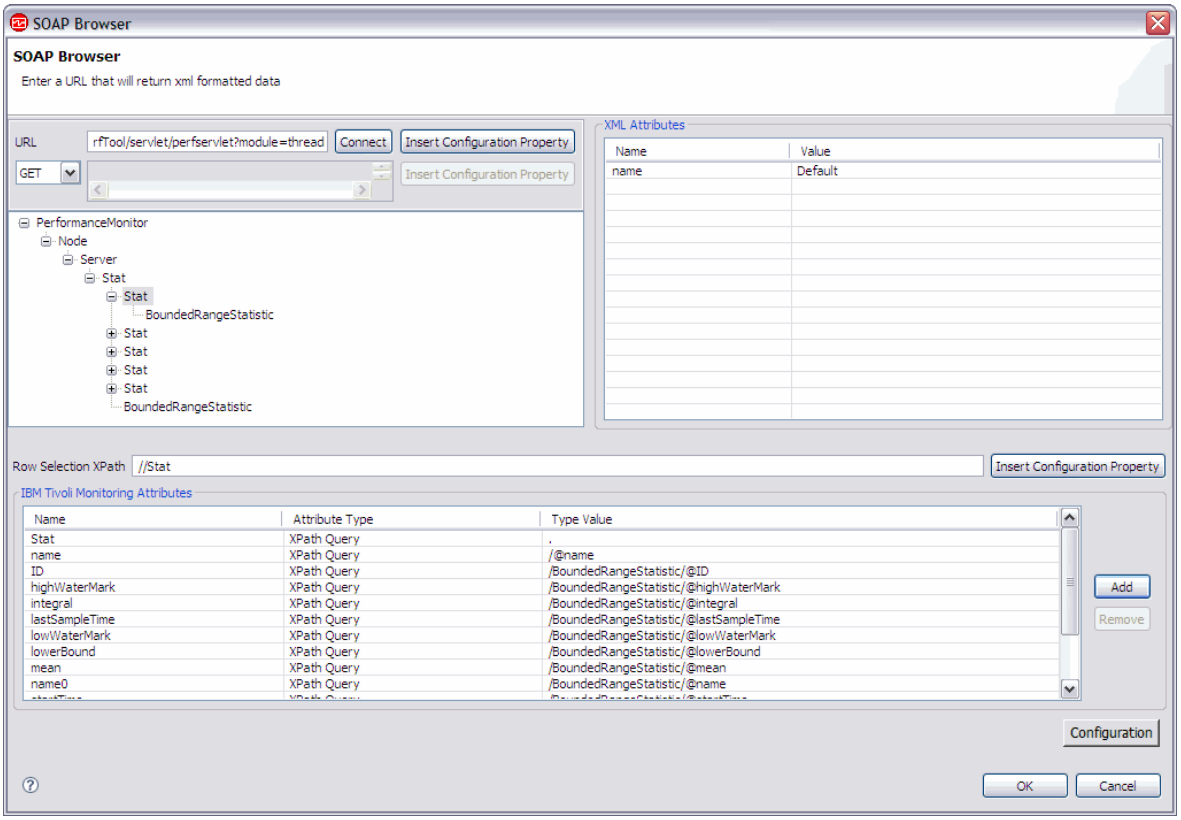


*Figura 46. Ventana **Navegador de SOAP***

f) En la ventana **Navegador de SOAP**, pulse **Aceptar** para guardar los cambios y volver a la ventana **Información de SOAP**.

8. En la ventana **Información de SOAP**, pulse **Siguiente**.
9. Si no ha utilizado **Examinar** anteriormente y ha especificado el **URL** y el **XPath de selección de filas** en la ventana **Información de SOAP**, se muestra la página **Información de atributos**. Especifique la información para el primer atributo en la página **Información de atributo**, y pulse **Finalizar**. A continuación, puede especificar más atributos utilizando Agent Editor. Para obtener más información sobre la creación de atributos, consulte "Creación de atributos" en la página 1230.
10. Si ha utilizado la función **Examinar** en el paso "6" en la página 1344, se muestra la página **Seleccionar atributos clave**. En la página **Seleccionar atributos clave**, seleccione los atributos clave o indique que este origen de datos solo produce una fila de datos. Para obtener más información, consulte el apartado "Selección de atributos clave" en la página 1208.
11. Opcional: Puede probar este grupo de atributos pulsando **Probar**. Para obtener más información sobre la prueba, consulte "Prueba de grupos de atributos de SOAP" en la página 1351
12. Opcional: Puede crear un filtro para limitar los datos que este grupo de atributos devuelve pulsando **Avanzado**. Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte "Filtrado de grupo de atributos" en la página 1239
13. Realice una de las acciones siguientes:
    a) Si utiliza el **Asistente de agente**, pulse **Siguiente**.
    b) Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.

Representación XML de datos JSON

Si la solicitud HTTP devuelve datos JSON, el proveedor de datos convierte los datos a XML.

El proveedor de datos convierte el nombre de un atributo JSON en el nombre del elemento. Para un atributo JSON de tipo simple, convierte el valor en datos de texto dentro del elemento. Los objetos JSON incorporados se convierten en elementos XML incluidos. Cualesquiera atributos subordinados se convierten en elementos subordinados.

El elemento XML raíz es `JSON_document`.

Si un nombre de atributo JSON contiene caracteres que no son válidos en un nombre de elemento, el proveedor de datos los modifica para generar un nombre de elemento válido. El proveedor de datos añade también un atributo `JSON_name` al elemento. El valor del atributo es el nombre de atributo JSON original.

Para cada elemento de una matriz JSON, el proveedor de datos crea un elemento XML `JSON_`*xxx*`_array_element`, donde *xxx* es el nombre de la matriz. El valor del elemento de matriz se convierte en texto en el elemento XML. Se añade un atributo `JSON_index` a cada elemento XML; el valor del atributo es el índice del elemento array dentro de la matriz.

El proveedor de datos añade los atributos siguientes a cada elemento:

- `JSON_level`: el nivel del nodo dentro del archivo JSON. La raíz del árbol representada por la etiqueta `JSON_document` es el nivel `1`.
- `JSON_type`: el tipo de nodo de JSON (object, array, string o number).

Campos específicos para atributos SOAP
En la ventana **Información de atributos**, hay dos campos para los atributos de SOAP que definen cómo se recopilan los datos desde la respuesta de SOAP.

El campo **Tipo de atributo** puede ser cualquier valor de una lista que controle la información sobre la respuesta que se ha devuelto. Algunos tipos de atributos requieren un valor en el campo **Valor de tipo**. El tipo de atributo predeterminado es XPath Query, que ejecuta una consulta de XPath en el contenido de la respuesta del servidor de SOAP. El valor de tipo es la consulta XPath que se está ejecutando. La siguiente tabla describe todos los tipos de atributo y el valor de tipo cuando se necesita uno:

Tabla 277. Información de atributos de SOAP

Tipo de atributo	Descripción	Valor de tipo	Tipo de datos devueltos	Diferencias con los protocolos FTP y de archivos
`XPath Query`	Ejecuta una consulta XPath en el contenido que se devuelve desde una conexión URL. La consulta se debe grabar para que devuelva datos útiles para un atributo, no una lista de nodos.	La consulta XPath que se ejecutará en el contenido que se obtiene desde una conexión URL. Si se ha definido una consulta de selección de filas, esta consulta de XPath debe ser relativa a la consulta de selección de filas.	Los datos que se devuelven pueden ser un valor de serie, un valor numérico o un valor de indicación de fecha y hora. El navegador de Agent Builder para SOAP detecta generalmente el tipo de datos correcto para el atributo a partir de los datos que se examinan. Si los datos están en formato DateTime de XML, puede especificar una indicación de fecha y hora como tipo de atributo y el agente convertirá el valor a Timestamp de Candle.	Ninguna

Tabla 277. Información de atributos de SOAP (continuación)

Tipo de atributo	Descripción	Valor de tipo	Tipo de datos devueltos	Diferencias con los protocolos FTP y de archivos
`Tiempo de respuesta`	La cantidad de tiempo en milisegundos que se ha tardado en descargar el contenido del URL solicitado.	Ninguna	Entero (número de milisegundos)	Ninguna
`Mensaje de respuesta`	El mensaje de respuesta de HTTP que devuelve el servidor.	Ninguna	Serie	El mensaje de respuesta se aplica solo si el URL utiliza protocolos HTTP o HTTPS.
`Código de respuesta`	El código de respuesta de HTTP que devuelve el servidor.	Ninguna	Entero	El código de respuesta se aplica solo si el URL utiliza protocolos HTTP o HTTPS. Siempre es 0 para los URL de archivos o de FTP.
`Longitud de respuesta`	El tamaño del contenido en bytes que se ha descargado desde el URL solicitado	Ninguna	Entero (tamaño en bytes)	Ninguna
`Cabecera de respuesta`	La cabecera de respuesta se puede utilizar para recuperar un valor de uno de los campos de cabecera de respuesta de URL. El argumento especifica qué campo es solicitado.	El campo de la cabecera de respuesta que se va a recopilar.	Serie	Normalmente los protocolos de archivo y FTP no tienen cabeceras que se puedan recopilar.

Tabla 277. Información de atributos de SOAP (continuación)				
Tipo de atributo	**Descripción**	**Valor de tipo**	**Tipo de datos devueltos**	**Diferencias con los protocolos FTP y de archivos**
`Solicitar URL`	La conexión se ha creado para este URL. Todas las palabras claves de respuesta proporcionan información sobre la conexión con este URL. La consulta XPath se puede utilizar para obtener información que se obtiene del contenido devuelto al acceder a este URL.	Ninguna	Serie	Ninguna

Opciones de XPath

Si utiliza el lenguaje XML Path, puede seleccionar nodos desde un documento XML. Algunos de los posibles usos de XPaths para los orígenes de datos de SOAP incluyen:

- Utilización de predicados en XPath para identificar los elementos XML que se corresponden a las filas de datos en el grupo de atributos de IBM Tivoli Monitoring. Puede utilizar predicados en XPath que correlacionen elementos XML o atributos con atributos de Tivoli Monitoring, como en el siguiente ejemplo:

  ```
  Stat[@name="URLs"]/CountStatistic[@name="URIRequestCount"]/@count
  ```

  Donde hay varios pasos de ubicación en XPath, cada uno de ellos puede contener uno o más predicados. Los predicados pueden ser complejos y contener valores booleanos u operadores de fórmula. Por ejemplo:

  ```
  //PerformanceMonitor/Node/Server[@name="server1"]/Stat/Stat/Stat[@name=
  "Servlets"]/Stat
  ```

- Inclusión de funciones de conjunto de nodos en el XPath, si una fila contiene varios elementos XML del mismo tipo. Y si la posición de un elemento XML en la lista de nodos determina el atributo de Tivoli Monitoring con el que se correlaciona el elemento. Ejemplos de funciones de conjunto de nodos son: `position()`, `first()`, `last()` y `count()`.
- Transformación de datos simple, como la subcadena. Si especifica la siguiente subcadena:

  ```
  substring(myXMLElement,1,3)
  ```

  el XPath devuelve los tres primeros caracteres del elemento XML, myXMLElement.

Puede especificar elementos fuera del contexto del XPath de selección de filas utilizando dos puntos seguidos, `(..`, como en el ejemplo siguiente:

```
/../OrganizationDescription/OrganizationIdentifier
```

Configuración de SOAP

Después de añadir el origen de datos de SOAP, la configuración se visualiza en la página **Configuración de tiempo de ejecución** de Agent Editor.

Se añaden las secciones de configuración para el servidor HTTP, para el servidor Proxy y para Java. Para obtener información sobre la configuración del servidor proxy, consulte "Configuración del servidor proxy" en la página 1342. Para obtener información sobre la configuración de Java, consulte "La configuración de Java" en la página 1342.

HTTP Server

La sección Configuración de servidor HTTP contiene las siguientes propiedades:

Tabla 278. Propiedades de configuración del servidor HTTP

Nombre	Valores válidos	Necesario	Descripción
Nombre de usuario HTTP	Serie	No	El usuario HTTP
Contraseña HTTP	Contraseña	No	La contraseña de servidor HTTP
Nombre de servidor HTTP	Serie (El valor predeterminado es localhost)	No	El host o dirección IP del servidor HTTP
Número de puerto HTTP	Numérico (El valor predeterminado es 80)	No	El host o dirección IP del servidor HTTP
Validación de certificados habilitada	True, False (El valor predeterminado es True)	Sí	La inhabilitación de la validación de certificados resulta potencialmente insegura
Archivo de almacén de confianza HTTP	Vía de acceso a un archivo	No	El archivo de almacén de confianza HTTP
Contraseña de almacén de confianza HTTP	La contraseña de almacén de confianza HTTP	No	La contraseña de almacén de confianza HTTP

Servidor proxy

Si el sistema en el que se está ejecutando el agente requiere un proxy para acceder al proveedor de datos SOAP, debe especificar las propiedades de configuración del servidor proxy. Para obtener más información, consulte el apartado "Configuración del servidor proxy" en la página 1342.

Prueba de grupos de atributos de SOAP

Puede probar el grupo de atributos de SOAP que ha creado, en Agent Builder

Procedimiento

1. El procedimiento de prueba se puede iniciar de las siguientes formas:
   - Durante la creación del agente, pulse **Probar** en la página **Información de SOAP**.
   - Tras la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** del Agent Editor y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208

   Tras pulsar **Probar** en uno de los dos pasos anteriores, se visualiza la ventana **Probar la recopilación de SOAP**.
2. Opcional: Antes de iniciar la prueba, puede establecer variables de entorno, propiedades de configuración e información de Java.

Para obtener más información, consulte “Prueba de grupo de atributos” en la página 1417. Si desea más información sobre la configuración de SOAP, consulte “Configuración de SOAP” en la página 1350.

3. Cambie el URL, el XPath de selección de filas y el tipo de solicitud.
4. Pulse **Iniciar agente**.

   Una ventana indica que el agente se está iniciando.
5. Para simular una solicitud de Tivoli Enterprise Portal o SOAP para los datos de agente, pulse **Recopilar datos**. Esta acción llena la tabla Resultados y puede obtener una vista previa de cómo se van a analizar y mostrar los datos en las columnas en Tivoli Enterprise Portal.

   En el área Resultados, puede cambiar las definiciones de atributos y volver a cargar los datos para ver cómo afectan los cambios al grupo de atributos. Puede pulsar con el botón derecho del ratón en el área de resultados de una columna para visualizar las opciones para editar el atributo. Las opciones de edición de atributos son:

   - **Editar atributo**
   - **Ocultar atributo**
   - **Insertar atributo antes**
   - **Insertar atributo después**
   - **Eliminar**
   - **Eliminar atributos siguientes**
   - **Eliminar todos**
6. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana **Estado de la recopilación de datos** recopila y muestra se describen en “Nodo Estatus de objeto de rendimiento” en la página 1462.
7. Detenga el agente pulsando **Detener agente**.
8. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Probar recopilación de SOAP**. Al pulsar **Aceptar** se guardan los cambios que ha realizado.

Conceptos relacionados

“Pruebas del agente en Agent Builder” en la página 1417
Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Supervisión de datos con un socket

Puede definir un origen de datos para recopilar datos de una aplicación externa utilizando un socket TCP. La aplicación debe iniciar la conexión TCP al agente y enviar datos en un formato XML estructurado. En función de la aplicación, el origen de datos puede producir un conjunto de datos con una sola fila, varias filas, o datos de sucesos.

Acerca de esta tarea

Utilice el origen de datos de socket para proporcionar datos al agente desde una aplicación externa, que se ejecuta en el mismo sistema que el agente. La aplicación externa puede enviar datos al agente en cualquier momento que lo desee. Por ejemplo, puede desarrollar una interfaz de línea de mandatos que permita a un usuario publicar datos en un grupo de atributos cuando se ejecute. Otra opción es modificar una aplicación supervisada para enviar actualizaciones al agente. El agente no inicia ni detiene la aplicación que envía datos al socket; esta acción está controlada por el usuario.

Existen algunas limitaciones para el origen de datos de socket:

- De forma predeterminada las conexiones con el host local (127.0.0.1) son posibles. Para obtener más información sobre cómo configurar el agente para que acepte conexiones de un host remoto, consulte “Conexión de puerto de socket remoto” en la página 1360.

- No hay ningún mecanismo en la API de socket para que el cliente determine qué subnodos están disponibles. El cliente puede enviar datos para un subnodo específico, pero debe conocer anteriormente el nombre del subnodo.

Utilice el procedimiento siguiente para crear un grupo de atributos para recopilar datos utilizando el socket TCP (protocolo de control de transmisiones).

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Programas personalizados** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **Socket**.
3. Pulse **Siguiente**.
4. En la página **Información de socket**, especifique un nombre de grupo de atributos.
5. Especifique un texto de ayuda para el grupo de atributos.
6. Seleccione si el grupo de atributos **Produce una sola fila de datos**, **Puede producir más de una fila de datos** o **Produce sucesos**. Para obtener más información, consulte el apartado "Envío de datos" en la página 1355.
7. En la sección Información sobre socket, seleccione **Página de códigos**. Para obtener más información, consulte el apartado "Juegos de caracteres" en la página 1358.
8. Opcional: Pulse **Avanzado** para modificar las propiedades avanzadas del grupo de atributos. La opción **Avanzado** está activa cuando se selecciona que el grupo de atributos **Puede producir más de una fila de datos** o **Produce sucesos**.
9. Pulse **Siguiente**.
10. En la página **Información de atributos**, especifique el primer atributo para el grupo de atributos. Para obtener más información sobre la creación de atributos, consulte "Creación de atributos" en la página 1230.
11. Pulse **Siguiente**.
12. Opcional: En la página **Información de origen de datos de socket global**, la sección **Códigos de error**, puede definir los códigos de error que puede enviar el cliente de socket cuando no puede recopilar datos. Para obtener más información, consulte ("Envío de errores en lugar de datos" en la página 1356). Para definir un código de error, siga estos pasos:

    a) En la sección **Códigos de error**, pulse **Añadir**. Un código de error tiene un límite de 256 caracteres. Sólo están permitidos las letras ASCII, los dígitos y los subrayados. No se permiten espacios.

    b) En la ventana **Definición del código de error de socket**, especifique un valor de visualización que se muestra en el grupo de atributos **Estado de objeto de rendimiento**.

    c) Especifique un valor interno. El valor interno debe ser un entero desde 1.000 a 2.147.483.647.

    d) Debe definir un texto del mensaje para cada error. Puede utilizar el texto de mensaje que se ha especificado previamente seleccionándolo en la lista. Pulse **Aceptar** para volver a la página **Información de origen de datos de socket global**. El texto del mensaje se utiliza en el archivo de registro del agente.

    Si no hay disponible ningún texto de mensaje adecuado, pulse **Examinar** para configurar el texto del mensaje. Se abre la ventana Mensajes (lista). La ventana de mensajes muestra una lista de los mensajes que están definidos en el agente. Hasta que defina mensajes, la lista permanece en blanco. Puede utilizar **Editar** para alterar un mensaje definido y **Eliminar** para suprimir uno o más mensajes que ha definido.

    e) En la ventana Mensajes (lista), pulse **Añadir** para ver una ventana **Definición de mensaje**. En la ventana **Definición de mensaje**, escriba el texto que describa el significado del nuevo mensaje y seleccione el tipo de mensaje.

    Nota: El identificador de mensaje se generará de forma automática.

    f) Pulse **Aceptar**.

g) Se abre la ventana Mensajes (lista), con el nuevo mensaje. Para verificar el mensaje y volver a la página **Información de origen de datos de socket global**, pulse **Aceptar**.

13. Opcional: En la sección **Archivos complementarios** de la página **Información de origen de datos de socket global**, puede añadir archivos que están empaquetados con el agente. Estos archivos se copian en el sistema del agente al instalarlo.

    La columna **Tipo de archivo** describe cómo espera utilizarse cada archivo. Se describen tres posibles usos en la siguiente tabla:

    Tabla 279. Tipos de archivos para archivos complementarios

Tipo de archivo	**Descripción**
Ejecutable	Seleccione esta opción si desea incluir un archivo ejecutable con el agente. El agente no utiliza estos archivos.
Biblioteca	Seleccione esta opción si desea incluir una biblioteca con el agente. El agente no utiliza estos archivos.
Recurso Java	Seleccione esta opción para incluir recursos Java con el agente. El agente no utiliza estos archivos.

    Para obtener información sobre dónde se instalan los archivos complementarios con el agente, consulte "Nuevos archivos en el sistema" en la página 1434.

    Pulse **Editar** para editar el archivo importado. Para obtener más información, consulte ("Edición de una definición de archivo de mandatos" en la página 1318).

14. Opcional: Puede probar este grupo de atributos pulsando **Probar**. Para obtener más información sobre pruebas, consulte "Prueba de grupos de atributos de socket" en la página 1362

15. Opcional: Si se muestrea el origen de datos, puede crear un filtro para limitar los datos que este grupo de atributos devuelve pulsando **Avanzado**. El origen de datos se muestrea cuando no se ha seleccionado "Produce sucesos" en la página **Información de socket**. Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte "Filtrado de grupo de atributos" en la página 1239

16. Realice una de las acciones siguientes:

    a) Si utiliza el **Asistente de agente**, pulse **Siguiente**.

    b) Pulse en **Finalizar** para guardar el origen de datos y abrir Agent Editor.

    Seleccione los sistemas operativos en los que el agente escucha los datos de los clientes de socket en la sección **Sistemas operativos** de la página **Valores de proveedor de sockets**. Para abrir la página, pulse **Valores de proveedor de sockets** en la vista de esquema o pulse **Valores globales** en Agent Editor en cualquier página de grupo de atributos de socket.

    Nota: Los códigos de error y los archivos complementarios se pueden actualizar en las secciones **Códigos de error** y **Archivos complementarios** de la página **Valores de proveedor de sockets**.

Envío de información de socket al agente

Cuando el agente contiene uno o más grupos de atributos de socket, el agente abre un socket y escucha datos desde los clientes.

La aplicación que envía los datos de socket al agente se conecta a un puerto que se define en el agente. El puerto es el valor que se establece mediante una propiedad de configuración de agente o un puerto efímero que TCP/IP asigna automáticamente. Para obtener más información sobre los puertos y la configuración de socket, consulte "Configuración del Socket" en la página 1359.

Los datos recibidos deben seguir un formato XML estructurado. Los siguientes flujos de información XML son posibles utilizando el origen de datos de socket:

- Enviar una o más filas de datos al agente para un grupo de atributos de muestra

- Enviar una fila de datos al agente para un grupo de atributos que Produce sucesos
- Enviar un código de error al agente en lugar de datos.
- Enviar un registro de prefijo de tareas al agente
- Recibir una solicitud de tareas desde el agente
- Enviar una respuesta de tareas al agente

Envío de datos

Un grupo de atributos se define para recibir datos de muestra o datos de suceso. Cuando cree el grupo de atributos, especifique una opción que indique si los datos que se recibirán:

- Produce una sola fila de datos
- Produce más de una fila de datos
- Produce sucesos

Si selecciona **Produce una única fila de datos** o **Puede producir más de una fila de datos**, es un grupo de atributos muestreados. Si selecciona **Produce sucesos**, el grupo de atributos envía un suceso al entorno de supervisión cada vez que se recibe una fila.

Al ver datos muestreados en Tivoli Enterprise Portal o la consola IBM Cloud Application Performance Management, verá el último conjunto de filas recopiladas. Los datos que se visualizan para un grupo de atributos de sucesos es el contenido de una memoria caché local que el agente mantiene. Para los datos de sucesos, el agente añade la nueva entrada a la memoria caché hasta que se alcance el tamaño cuando se suprima la más antigua. Para datos de muestra, el agente sustituye el contenido de la memoria caché cada vez que envía datos.

Si selecciona **Produce sucesos** o **Produce una única fila de datos**, solo debe enviar una fila de datos al agente para el grupo de atributos de cada mensaje. Puede enviar tantos sucesos como desee, pero envíe cada suceso en un mensaje separado.

Normalmente, los datos de ejemplo los recopila el agente a petición, pero el cliente de socket proporciona muestras actualizadas con su propia planificación. Puede actualizar un grupo de atributos de muestra (una sola fila o varias filas) tan a menudo como sea necesario. Cuando Tivoli Monitoring o IBM Cloud Application Performance Management solicita los datos, el agente proporciona los últimos datos.

Si faltan filas de datos para el grupo de atributos de socket en Tivoli Enterprise Portal o la consola IBM Cloud Application Performance Management, compruebe los errores del archivo de registro. Además, si los datos del grupo de atributos no son los esperados, compruebe si hay errores en el archivo de registro. El origen de datos de socket intentará procesar todo lo que pueda de la entrada. Por ejemplo, si el cliente envía tres filas bien formadas y una no es válida (por ejemplo, XML incorrectamente formado), verá:

- Tres filas de datos en el grupo de atributos
- Se registra un error para la fila incorrectamente formada en el archivo de registro del agente
- Puesto que se han devuelto filas válidas, el Estado de objeto de rendimiento muestra el estado `NO_ERROR`

Para datos de sucesos y muestreados, los datos se envían al agente como un único flujo de datos XML desde el cliente de socket. Los datos que se envían desde un cliente de socket siempre deben terminarse con un carácter de nueva línea: `'\n'`. El agente lee los datos hasta que ve el carácter de salto de línea y se realiza un intento de procesar lo que se ha recibido. Cualquier dato recibido que no se pueda procesar se descarta. A continuación se muestra un ejemplo de cómo podría enviar dos filas de datos al agente para un grupo de atributos denominado `abc`:

```
<socketData><attrGroup name="abc"><in><a v="1"/><a v="no"/><a v="5"/></in><in> \
<a v="3"/><a v="yes"/><a v="5"/></in></attrGroup></socketData>\n
```

Esta muestra envía dos filas de datos al agente donde cada fila contiene tres atributos. El orden de los atributos es importante y debe seguir el orden definido en el grupo de atributos. La única excepción a esto es que se deben saltar los atributos derivados, independientemente de dónde se encuentren en el grupo de atributos.

Si el grupo de atributos está definido en un subnodo, el ID de instancia de subnodo debe identificarse cuando se envían datos al agente. El ID de instancia de subnodo se identifica utilizando el atributo de subnodo en el elemento `socketData`. Debe adoptarse una convención para configurar ID de instancias de subnodo para que la utilice el cliente de socket, dado que el cliente no puede consultar ID de instancia ni propiedades de configuración. Los datos enviados a un subnodo que no está configurado se ignorarán.

A continuación se muestra un ejemplo:

```
<socketData subnode="app1"><attrGroup name="abc"><in><a v="1"/><a v="no"/><a v="5"/>
</in><in> \<a v="3"/><a v="yes"/><a v="5"/></in></attrGroup></socketData>\n
```

En este ejemplo, los datos se envían al subnodo con un ID de instancia igual a `"app1"`. `"app1"` no es el nombre del sistema gestionado, sino el identificador de instancia que se especifica cuando se configura la instancia de subnodo.

Los siguientes elementos XML configuran los datos de socket:

socketData
El elemento raíz. Tiene un atributo opcional denominado `subnode` que especifica el ID de instancia de subnodo.

attrGroup
Este elemento identifica el grupo de atributos para el que se destinan los datos de socket. El atributo `name` es necesario y se utiliza para especificar el nombre de grupo de atributos.

in
Este elemento es necesario para identificar una nueva fila de datos. Todos los valores de atributos para una fila de datos deben ser hijos del mismo elemento `in`.

a
El elemento a identifica un valor de atributo. El atributo `v` es necesario y se utiliza para especificar el valor de atributo.

Envío de errores en lugar de datos

A veces, puede que la aplicación que publica datos de socket no pueda recopilar los datos necesarios para un grupo de atributos. En este caso, en lugar de enviar datos al agente, se puede devolver un código de error. El código de error le proporciona una forma de notificar al entorno de supervisión su problema. Un error de ejemplo es:

```
<socketData><attrGroup name="abc"/><error rc="1000"/></attrGroup></socketData>\n
```

El código de error debe estar definido en el agente en una lista que es común a todos los grupos de atributos de socket. Cuando el agente reciba un código de error, el mensaje de error definido se registrará en el archivo de registro del agente. Además, el grupo de atributos denominado Estado de objeto de rendimiento tiene un atributo Código de error que se actualiza con el Tipo de código de error. El Tipo de código de error se define para el código de error que se envía.

Para el ejemplo anterior, debe definir el Valor de código de error 1000 en el agente. Consulte la siguiente definición de código de error de muestra:

Tabla 280. Código de error de muestra

Valor de código de error	Tipo de código de error	Mensaje
1000	APP_NOT_RUNNING	La aplicación no se está ejecutando

Cuando se envía el código de error, se registra un mensaje similar al siguiente en el archivo de registro del agente:

```
(4D7FA153.0000-5:customproviderserver.cpp,1799,"processRC") Código de error 1000
 del cliente. \Mensaje: K1C0001E La aplicación no se está ejecutando
```

Si selecciona la consulta Estado de objeto de rendimiento en Tivoli Enterprise Portal, la columna **Código de error** para el grupo de atributos **abc** muestra el valor APP_NOT_RUNNING en esa tabla.

El envío de un error a un grupo de atributos de ejemplo borra cualquier dato que se recibiera anteriormente para dicho grupo de atributos. El envío de datos al grupo de atributos hace que el código de error no se siga mostrando en el grupo de atributos Estatus de objeto de rendimiento. También puede enviar un código de error de 0 para borrar el código de error de dicha tabla.

Cuando se envía un error a un grupo de atributos que produce sucesos, no se borra la memoria caché de sucesos que se han enviado previamente.

Manejo de solicitudes de actuación

El cliente de socket puede registrarse para recibir solicitudes de actuación del agente cuando el mandato de acción coincida con determinado prefijo. Cualquier acción que no coincida la manejará el agente. El prefijo no debe entrar en conflicto con las acciones que espera manejar el agente, por lo que utilice el código de producto del agente como el prefijo. Las actuaciones proporcionadas con Agent Builder tienen el nombre del origen de datos que la actuación utiliza. Por ejemplo, la actuación JMX_INVOKE opera en el origen de datos JMX. Otro ejemplo es la actuación SSHEXEC que utiliza el proveedor de datos del script SSH. Como estas acciones no utilizan el código de producto, este es un prefijo seguro para utilizarlo como prefijo de la actuación.

El cliente de socket debe ser de larga ejecución y dejar abierto el socket. Debe enviar una solicitud de registro para el prefijo y escuchar solicitudes desde el socket. El agente asegura que no se produce un tiempo de espera excedido en el socket de un cliente de larga ejecución, incluso si no fluyen datos. A continuación se muestra una consulta de registro de muestra:

```
<taskPrefix value="K42"/>\n
```

En este ejemplo, cualquier mandato actuación que el agente reciba que comience por "K42" se reenvía al cliente de socket que ha iniciado el registro. A continuación se muestra una solicitud de actuación que el cliente de socket puede recibir:

```
<taskRequest id="1"><task command="K42 refresh" user="sysadmin"/></taskRequest>\n
```

El id es un identificador exclusivo que el agente utiliza para rastrear consultas que se envían a los clientes. Cuando el cliente de socket responde a la tarea, debe proporcionar este identificador en el atributo id del elemento taskResponse.

El cliente de socket debe procesar la acción y enviar una respuesta. Una respuesta de muestra sería:

```
 <taskResponse id="1" rc="1"/>\n
```

Si la acción finaliza correctamente, se devolverá un valor de atributo rc de 0. El valor de rc debe ser un entero, en el que cualquier valor distinto de 0 se considera como un error. El valor de código de retorno de la tarea se registra en el archivo de registro del agente y se muestra en la consulta Estatus de actuación que se incluye con el agente. El diálogo que se muestra en Tivoli Enterprise Portal después de que se ejecuta una acción no muestra el código de retorno. Este diálogo indica si el mandato de actuación ha devuelto éxito o error. Se debe visualizar el registro de agente o la consulta de Estatus de actuación para determinar el código de retorno real si se ha producido un fallo.

Es responsabilidad del desarrollador del agente documentar, crear e importar cualquier acción que esté soportada por los clientes de socket que se utilizan con un agente. Si los usuarios envían acciones no soportadas al cliente de socket, el cliente debe estar desarrollado para manejar dichos casos de ejemplo de forma adecuada. Si los usuarios definen más acciones que empiezan por el prefijo registrado, se pasan al cliente. El cliente debe estar desarrollado para manejar estos escenarios de manera adecuada.

Hay un tiempo de espera que controla cuanto tiempo espera el agente una respuesta del cliente de socket. El valor es una variable de entorno que se define en el agente denominado CDP_DP_ACTION_TIMEOUT y el valor predeterminado es 20 segundos.

Nota: Los mensajes de código de error que se definen para los grupos de atributos de origen de datos de socket no se utilizan para las actuaciones. Puede devolver los mismos valores de código de retorno. Sin

embargo, el agente no registra el mensaje que se ha definido o afecta el campo `Código de error` en el grupo de atributos Estatus de objeto de rendimiento.

Codificación de datos de socket
El cliente de socket codifica los datos que se envían al agente.

Es importante ser consciente de cómo el cliente de socket codifica los datos que se envían al agente.

Caracteres especiales

Los datos enviados al agente no deben contener ningún carácter de salto de línea, a excepción del final de cada ejemplo de suceso o de datos. Los caracteres de nueva línea que aparecen dentro de valores de atributo deben sustituirse por un carácter o codificación diferente tal como se muestra en la Tabla 281 en la página 1358. También debe tener cuidado de no interrumpir la sintaxis XML con valores de atributos. La tabla siguiente muestra los caracteres que aparecen en los valores de atributo que se codifican:

Tabla 281. Caracteres a codificar en valores de atributo

Carácter	**Cabecera**
&	`&`
<	`<`
>	`>`
“	`"`
'	`'`
\n	`
`

Nota: El agente utiliza el carácter de salto de línea para separar las respuestas recibidas de un cliente. Los caracteres de línea nueva inesperados impiden analizar los datos correctamente.

El agente no contiene un analizador XML completo, por lo que no debe utilizar codificación especial para caracteres que no se encuentran en la Tabla 281 en la página 1358. Por ejemplo, no codifique `¢` ni `&cent` en lugar de un signo de centavos ¢.

Juegos de caracteres

Además de codificar los caracteres especiales, el agente debe saber qué página de código se ha utilizado para codificar los datos. Defina cada grupo de atributos de socket para indicar si envía los datos al agente como datos **UTF-8** o como **Página de códigos local**. Tenga presente cómo está enviando datos su cliente. Si utiliza un cliente que está escrito en Java, especifique **UTF-8** como la codificación en el grabador que utilice para enviar datos al agente. Especifique **UTF-8** como **Página de códigos** para el grupo de atributos. **Página de códigos local** indica la página de códigos local del agente. Si los datos se envían por un socket remoto, debe ajustarse a la página de códigos local del agente o utilizar UTF-8.

Datos numéricos

Tenga presente cómo está formateando los valores de atributos numéricos. Los valores numéricos que envíe al agente no deben contener ningún carácter especial. Un ejemplo es el carácter separador de millares. Otros ejemplos son los símbolos de moneda o los caracteres que describen las unidades del valor. Si el agente encuentra un problema cuando está analizando datos numéricos, registra un error que indica el problema. El Código de error de estatus de objeto de rendimiento no se establece cuando falla el análisis de un atributo. A continuación se muestra un mensaje de error de ejemplo del registro del agente:

```
(4D3F1FD6.0021-9:utilities.cpp,205,"parseNumericString") Caracteres no válidos :00:04 \
encontrados al obtener el valor numérico desde 00:00:04, que devuelve 0.000000
```

Nota: Para obtener información sobre cómo el atributo de indicación de fecha y hora debe estar formateado, consulte “Indicación de fecha y hora” en la página 1236.

Errores de socket
Los errores se grabarán en el archivo de registro del agente para problemas que se produzcan con datos recibidos desde un cliente de socket.

Otros errores que se registran son `actuaciones` que devuelven un valor distinto de `0`. Los valores de error que el cliente de socket envía se registran junto con el mensaje asociado al código de error.

El Estatus de objeto de rendimiento para el grupo de atributos se establece cuando el cliente de socket envía un código de retorno de error al agente. Se pueden ver algunos otros valores además de los definidos por el agente. La tabla siguiente describe otros valores de "Código de error" que puede encontrar con los grupos de atributos de socket:

Tabla 282. Valores del Estado de objeto de rendimiento

Código de error	**Descripción**
NO_ERROR	No se ha producido ningún error. Indica que no hay ningún problema con el grupo de atributos. Los problemas con una fila de datos muestreados no hacen que cambie el estado NO_ERROR. Debe validar el número de filas que se muestran y los valores de atributo incluso cuando vea NO_ERROR como código de error.
NO_INSTANCES_RETURNED	Un cliente de socket no envió filas de datos para un grupo de atributos de muestra. No es un error. Indica que no hay ninguna instancia de los recursos supervisados por este grupo de atributos.
XML_PARSE_ERROR	El agente no ha podido analizar los datos que se reciben del cliente. Consulte el registro del agente para obtener más detalles.
OBJECT_CURRENTLY_UNAVAILABLE	El cliente envió al agente un código de error que no estaba definido en la lista global de códigos de error.
GENERAL_ERROR	Se ha producido un problema al recopilar datos del cliente, normalmente debido a que el cliente no respondió a la consulta dentro del intervalo del tiempo de espera. Consulte el registro del rastreo de agente para obtener más detalles. El cliente también puede especificar GENERAL_ERROR como código de error, pero es mejor si se define un código de error más detallado.

Configuración del Socket
Después de añadir un origen de datos de socket al agente, puede configurar el agente para que acepte datos de un puerto de socket especificado.

Acerca de esta tarea

Después de añadir un origen de datos de socket, la configuración se visualiza en la página **Configuración de tiempo de ejecución** de Agent Editor. La sección de configuración de Socket contiene la siguiente propiedad:

Tabla 283. Propiedad de configuración del socket			
Nombre	**Valores válidos**	**Necesario**	**Descripción**
Número de puerto	0 o cualquier entero positivo El valor predeterminado es 0	Sí	El puerto que el agente utiliza para escuchar los datos de los clientes de socket. El valor 0 indica que se debe utilizar un puerto efímero.

El agente graba el valor del puerto que se está utilizando en un archivo. Los clientes de socket que se ejecutan en el sistema del agente pueden leer más tarde este archivo para determinar a qué puerto conectarse. El archivo en el que se graba el puerto se denomina *kxx_nombre_instancia*_cps.properties, donde: *kxx* es el código de tres caracteres del producto del agente y *nombre_instancia* es el nombre de la instancia de agente para un agente de varias instancias. Si el agente no es un agente de varias instancias, esta parte del nombre no se incluye, por lo que el nombre de archivo es *kxx*_cp.properties.

En Windows, el archivo se graba en el directorio %CANDLE_HOME%\TMAITM6 para las instalaciones de 32 bits o en %CANDLE_HOME%\TMAITM6_x64 para las instalaciones de 64 bits. EnUNIX, el archivo se graba en /tmp.

Procedimiento

1. Opcional: Establezca la variable de entorno CDP_DP_HOSTNAME en el nombre de host o dirección IP de la interfaz de red, si el sistema tiene varias interfaces:
   a) Vaya a la vista Información de agente de **Agent Editor** y seleccione **Variables de entorno**.
   b) Pulse **Añadir** y seleccione CDP_DP_HOSTNAME en la lista de variables de entorno, utilizando el campo Nombre.
   c) Establezca el nombre de host o la dirección IP en el campo Valor.
2. Inicie el agente.

   Cuando se inicia el agente, se enlaza a la interfaz definida por la variable de entorno CDP_DP_HOSTNAME. Si CDP_DP_HOSTNAME no se establece, el agente se enlaza al nombre de host predeterminado.

   Si desea que el agente se enlace a un puerto definido en lugar de a un puerto efímero, puede establecer la propiedad de configuración **Número de puerto** (CP_PORT).

   Para establecer la propiedad de configuración de número de puerto, siga estos pasos:

   a) Vaya a la vista Agent Editor **Configuración de tiempo de ejecución**.
   b) En el panel **Información de configuración de tiempo de ejecución**, seleccione **Configuración para Socket** > **Socket** > **Número de puerto**
   c) Entre un valor de número de puerto en **Valor predeterminado**.
      Si no entra un valor, se utiliza 0. El valor 0 india que se utiliza un puerto efímero.

Conexión de puerto de socket remoto

Puede configurar al agente para que acepte los datos de un puerto de socket remoto. El agente debe ejecutarse en un sistema que posea una conexión de interfaz de red a un sistema remoto.

Procedimiento

1. Siga los pasos a continuación para establecer el valor de la variable de entorno CDP_DP_ALLOW_REMOTE en YES.
   a) Vaya a la página **Información de agente** de Agent Editor y seleccione **Variables de entorno**.

b) Pulse **Añadir** y seleccione CDP_DP_ALLOW_REMOTE en la lista de variables de entorno utilizando el campo **Nombre**.

c) Establezca el campo **Valor** en YES.

2. Siga el procedimiento que se detalla en "Configuración del Socket" en la página 1359.

Restricción:

- Los datos que se envían entre la aplicación de socket y el agente:
  - Deben ajustarse a la sintaxis XML definida para el proveedor de datos de socket. Para obtener más información, consulte " Codificación de datos de socket" en la página 1358.
  - Deben estar codificados en UTF-8.
  - Se envía en texto simple (sin cifrar). Si los datos contienen información confidencial, la comunicación debe protegerse mediante un túnel SSH u otro mecanismo fuera del agente.
- El agente procesa datos recibidos desde cualquier host remoto, por lo que el entorno debe protegerse con el cortafuegos o los filtros de tráfico de red adecuados.

Resultados

Puede ejecutar un código que implemente un proveedor de datos de socket en cualquier sistema que pueda conectarse al sistema donde se ejecuta el agente.

Script de muestra para el socket

Este script de muestra presenta cómo se puede escribir un cliente de socket.

Muestra de Perl

El siguiente script de Perl de muestra conecta a un socket y envía datos. Este ejemplo se ha escrito para un agente que se ejecuta en UNIX, con el código de producto k00 y un grupo de atributos denominado SocketData.

```
#!/usr/bin/perl -w
# SocketTest.pl
# A simple Agent Builder Socket client using IO:Socket
#------------------------

use strict;
use IO::Socket;

# Initialize socket connection to the agent
#----------------------
my $host = '127.0.0.1';
my $port = 0;
# This sample is for an agent with the k00 product code.  The product code is
# used in the following line to find the file containing the port number to use.
open PORTFILE, "/tmp/k00_cps.properties" || die "Port file not found $!\n";
while (<PORTFILE>) {
    if (/^CP_PORT=([0-9]+)/) {
        $port = $1;
    }
}

if ($port == 0) {
    die "Could not find port to use to connect to agent.\n";
}

my $sock = new IO::Socket::INET( PeerAddr => $host, PeerPort => $port,
Proto => 'tcp'); $sock or die "no socket :$!";

# The following call sends 2 rows of data to the agent.  Each row contains 1
# String attribute and 3 numeric attributes.
syswrite $sock, "<socketData><attrGroup name=\"SocketData\"><in><a v=\"A message
from perl\"/>  \<a v=\"1\"/><a v=\"2\"/><a v=\"123\"/></in><in><a v=\"More from
perl\"/><a v=\"456\"/>  \<a v=\"123\"/><a v=\"789\"/></in></attrGroup>
</socketData>\n";

close $sock;
```

Prueba de grupos de atributos de socket

Puede probar el grupo de atributos de socket que ha creado, en Agent Builder.

Antes de empezar

Para probar el grupo de atributos, se necesita un cliente de socket para enviar datos. Puede ver un ejemplo de cliente de socket que está escrito con script de Perl en "Script de muestra para el socket" en la página 1361

Restricción: A diferencia de la mayoría de los demás grupos de atributos, no puede probar el grupo de atributos de socket mientras se está creando. Puede probar el grupo de atributos cuando se complete su creación.

Procedimiento

1. Seleccione un grupo de atributos en la página **Definición de origen de datos** de Agent Editor después de la creación del agente y pulse **Probar** . Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208.

   Después de pulsar **Probar** en uno de los dos pasos anteriores, se visualiza la ventana **Probar cliente de socket**.
2. Opcional: Establezca las variables de entorno y las propiedades de configuración antes de iniciar la prueba.

   Para obtener más información, consulte "Prueba de grupo de atributos" en la página 1417.
3. Pulse **Iniciar agente**. Una ventana indica que el agente se está iniciando.
4. Cuando el agente se inicia, escucha datos de socket según su configuración.
5. Para probar la recopilación de datos del agente, debe generar ahora datos de socket que coincidan con la configuración de los agentes.

   Puede generar datos de socket utilizando un cliente de socket.

   Cuando el agente recibe datos de socket que coinciden con su configuración, añade los datos a su memoria caché interna.
6. Para simular una solicitud de Tivoli Enterprise Portal para los datos de agente, pulse **Recopilar datos**.

   La ventana **Probar cliente de socket** recopila y muestra los datos de la memoria caché del agente desde que se inició por última vez.
7. Pulse **Comprobar resultados** si algo parece no estar funcionando como se esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana Estado de la recopilación de datos recopila y muestra se describen en "Nodo Estatus de objeto de rendimiento" en la página 1462
8. Detenga el agente pulsando **Detener agente**.
9. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Probar cliente de socket**. Al pulsar **Aceptar** se guardan los cambios que ha realizado.

Conceptos relacionados

"Pruebas del agente en Agent Builder" en la página 1417
Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Utilización de la API de Java para supervisar datos

Puede definir un origen de datos para utilizar la API de Java para interactuar con una aplicación de larga ejecución en la plataforma Java. El agente inicia la aplicación al inicio e interactúa con ella de forma periódica. Cuando crea el agente, Agent Builder crea el código fuente de la aplicación. Debe personalizar el código para recopilar los datos correctos. En función del código, el origen de datos puede producir varios conjuntos de datos que pueden contener una sola fila, varias filas o datos de sucesos.

Acerca de esta tarea

Utilice el origen de datos de la API de Java y el lenguaje de programación Java para recopilar datos que no se pueden recopilar utilizando otros orígenes de datos de Agent Builder. El agente comienza la aplicación Java y envía una consulta de cierre cuando es hora de cerrarse. La aplicación Java debe salir solo cuando se le solicite hacerlo.

Un agente que contiene grupos de atributos de la API de Java interactúa con el proceso de aplicación Java. La aplicación Java utiliza la API de cliente del proveedor de Java para interactuar con el agente. Para obtener más información acerca de la API, consulte el Javadoc en el Tivoli Monitoring Knowledge Center. Con la API de Java puede:

- Conectar al proceso del agente y registrar los grupos de atributos soportados por la aplicación Java
- Recibir y responder a una consulta para datos de muestra
- Enviar datos de forma asíncrona para un grupo de atributos que produce sucesos
- Enviar un error para un grupo de atributos donde la recopilación de datos está fallando
- Soportar los grupos de atributos en subnodos con instancias de subnodos configuradas
- Recibir y responder a una solicitud de "Actuación"

Utilice el siguiente procedimiento para crear un grupo de atributos que recopile datos en una aplicación Java y los envíe utilizando la API de Java. El procedimiento muestra cómo crear una aplicación Java de muestra para utilizarla como punto de partida para la aplicación Java.

Procedimiento

1. En la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**, pulse **Programas personalizados** en el área **Categorías de datos de supervisión**.
2. En el área **Orígenes de datos**, pulse **API de Java**.
3. Pulse **Siguiente**.
4. En la página **Información de API de Java**, entre un nombre de grupo de atributos.
5. Especifique un texto de ayuda para el grupo de atributos.
6. Seleccione si el grupo de atributos **Produce una sola fila de datos**, **Puede producir más de una fila de datos** o **Produce sucesos**. Esta opción afecta la aplicación Java de muestra que se crea al final del asistente. Para obtener más información, consulte el apartado “Envío de datos” en la página 1355.
7. Opcional: Pulse **Avanzado** para modificar las propiedades avanzadas del grupo de atributos. **Avanzado** está disponible cuando se selecciona que el grupo de tributos **Puede producir más de una fila de datos** o **Produce sucesos**.
8. Pulse **Siguiente**.
9. En la página **Información de atributo**, especifique el primer atributo para el grupo de atributos. Para obtener más información sobre la creación de atributos, consulte “Creación de atributos” en la página 1230.
10. Seleccione **Añadir atributos adicionales** y pulse **Siguiente** para añadir otros atributos al agente. Las referencias a los atributos se incorporan en la aplicación Java de muestra que se crea al final del asistente.
11. Pulse **Siguiente**.
12. En la página **Información de origen de datos de la API de Java global**, entre un nombre de clase y un nombre de archivo JAR.

    El nombre de clase es un nombre de clase cualificado cuyo método principal se llama cuando se inicia Java. La aplicación Java de muestra se crea con el método Java principal en esta clase.

    El archivo JAR es el archivado que contiene las clases Java que componen la aplicación Java. El archivo JAR está empaquetado con el agente y se instala con él.
13. Opcional: Defina los códigos de error que la aplicación Java puede enviar, en la página **Información de origen de datos de API de Java global**, sección **Códigos de error**. La aplicación Java envía estos códigos de error cuando no puede recopilar datos.

Restricción: Un código de error tiene un límite de 256 caracteres. Sólo están permitidos las letras ASCII, los dígitos y los subrayados. No se permiten espacios.

a) Pulse **Añadir** en la sección Códigos de error.

b) En la ventana **Definición de código de error de la API de Java**, entre un valor de visualización.

c) Especifique un valor interno. El valor interno debe ser un entero desde 1.000 a 2.147.483.647.

d) Defina un texto de mensaje para cada error. Puede utilizar el texto de mensaje que se ha especificado previamente seleccionándolo en la lista. Pulse **Aceptar** para volver a la página **Información de origen de datos de la API de Java global**.

El mensaje se registra en el archivo de registro del agente.

e) Si no hay disponible ningún texto de mensaje adecuado, pulse **Examinar** para configurar el texto del mensaje.

Se visualiza la ventana Los mensajes (lista). La ventana de mensajes muestra una lista de los mensajes que están definidos en el agente. Hasta que defina mensajes, la lista permanece en blanco. Puede utilizar **Editar** para alterar un mensaje definido y **Eliminar** para suprimir uno o más mensajes que ha definido.

f) En la ventana Mensajes (lista), pulse **Añadir** para ver una ventana **Definición de mensaje**. En la ventana **Definición de mensaje**, puede escribir el texto que describe el significado del nuevo mensaje y seleccionar el tipo de mensaje.

Nota: El identificador de mensaje se generará de forma automática.

g) Pulse **Aceptar**.

h) Aparecerá la ventana Mensajes (lista) con el nuevo mensaje. Para verificar el mensaje y volver a la página **Información de origen de datos de la API de Java global**, pulse **Aceptar**.

14. Opcional: En la sección **Archivos complementarios** de la página **Información de origen de datos de la API de Java global**, puede añadir archivos que se empaquetan con el agente y se copian en el sistema del agente en la instalación del agente. El archivo JAR de la API de cliente del proveedor de Java no se lista aquí; se copia automáticamente en el sistema del agente. La columna **Tipo de archivo** describe cómo espera utilizarse cada archivo. En la tabla siguiente, se describen tres posibles usos (Tabla 284 en la página 1364). Pulse **Editar** para editar el archivo importado. Para obtener más información, consulte (“Edición de una definición de archivo de mandatos” en la página 1318).

Tabla 284. Tipos de archivos para archivos complementarios

Tipo de archivo	**Descripción**
Ejecutable	Seleccione esta opción si desea incluir un archivo ejecutable con el agente. El agente no utiliza este archivo, pero se encuentra en la vía de acceso para que lo utilice la aplicación Java.
Biblioteca	Seleccione esta opción si desea incluir una biblioteca con el agente. El agente no utiliza este archivo, pero se encuentra en la vía de acceso de la biblioteca para que la aplicación Java lo utilice.
Recurso Java	Seleccione esta opción para incluir recursos Java con el agente. El agente no utiliza este archivo, pero se encuentra en la vía de acceso de clase para que la aplicación Java lo utilice.

Nota: Cuando se añade un archivo complementario de recursos de Java al Agent Builder, el archivo se añade automáticamente a la vía de acceso de clases del proyecto. El compilador de Java utiliza el archivo complementario para resolver cualquier referencia que tenga el código, a clases en el recurso.

Para obtener información sobre dónde se instalan los archivos complementarios con el agente, consulte "Nuevos archivos en el sistema" en la página 1434.

15. Opcional: Cree un filtro para limitar los datos devueltos por este grupo de atributos, si los datos son muestreados. Cree un filtro pulsando **Avanzado**.

    Nota: Los datos se muestrean si no ha seleccionado **Produce sucesos** en la página **Información de API de Java**.

    Para obtener más información sobre el filtrado de datos desde un grupo de atributos, consulte "Filtrado de grupo de atributos" en la página 1239.

16. Opcional: Añada propiedades de configuración al subnodo.

    Si añade este origen de datos a un subnodo, la página **Alteraciones temporales de configuración de subnodo** se visualiza para que pueda añadir propiedades de configuración al subnodo. Se necesita por lo menos una propiedad de configuración bajo el subnodo para crear la aplicación Java de muestra. Se necesita por lo menos una propiedad de configuración porque el ejemplo utiliza una propiedad de configuración para distinguir una instancia de subnodo de otra.

17. Realice una de las acciones siguientes:

    a) Si utiliza el **Asistente de agente**, pulse **Siguiente**. Complete el asistente según sea necesario.

    b) De lo contrario, pulse **Finalizar** para guardar el origen de datos y abrir Agent Editor. A continuación, en el menú principal, seleccione **Archivo** > **Guardar**.

    En este punto, Agent Builder crea el código fuente para la aplicación de supervisión. El código está ubicado en el subdirectorio `src` del directorio del proyecto. Edite este código para crear la aplicación de supervisión.

Qué hacer a continuación

Seleccione los sistemas operativos correctos en la página **Valores de la API de Java**. Realice esta selección si este grupo de atributos y la aplicación Java se ejecutan en diferentes sistemas operativos a los sistemas operativos definidos para el agente. Para abrir la página, pulse **Valores de API de Java** en la vista esquema o pulse **Valores globales** en Agent Editor en cualquier página de grupo de atributos de la API de Java.

Nota: Los códigos de error y los archivos complementarios pueden actualizarse más adelante en las secciones **Códigos de error** y **Archivos complementarios** de la página **Valores de la API de Java**.

Ejecución de la aplicación Java

Información sobre la inicialización de la aplicación Java y sus dependencias

Inicialización de la aplicación Java

El agente inicia la aplicación Java mientras que el agente está iniciándose e inicializándose. Los valores de configuración se utilizan para controlar qué tiempo de ejecución Java se utiliza para iniciar el proceso. Los argumentos de la máquina virtual de Java y el nivel de registro de Java también se pueden especificar en la configuración. Si desea más información sobre la configuración de la API Java, consulte "Configuración de la API de Java" en la página 1375. El proceso de Java hereda las variables de entorno que se definen para el agente. Los valores de configuración de tiempo de ejecución se colocan también en el entorno y se pueden consultar utilizando llamadas de la API.

La aplicación Java debe ser un proceso de larga ejecución. No debe terminar a menos que reciba una solicitud de conclusión de la API. Si la aplicación Java termina después de registrarse en el agente, este intentará reiniciar la aplicación Java hasta tres veces. Si la recopilación de datos se reanuda satisfactoriamente, el recuento de reinicio se restablecerá. El agente registrará un error cuando una aplicación Java finalice y cuando se inicie un reinicio.

Nota: Si la aplicación Java finaliza antes de que se complete el registro del grupo de atributos, no se intentará un reinicio.

Dependencias

Una aplicación Java debe utilizar un entorno de tiempo de ejecución de Java. Las siguientes versiones de Java están soportadas:

- Oracle Corporation Java Versión 5 o posterior
- IBM Corporation Java Versión 5 o posterior

Java ya debe estar instalado en el sistema del agente cuando éste se haya configurado e iniciado. El archivo JAR que contiene la API utilizada para comunicarse con el agente se incluye con el agente `runtime` y en `classpath` de la JVM. Cualquier archivo JAR adicional que la aplicación Java necesite debe definirse como archivo suplementario para los grupos de atributos de la API de Java. Cualquier archivo complementario que tenga un *Tipo de archivo* de *Recurso Java* se añade automáticamente a la `classpath` base de la aplicación Java, junto con el archivo JAR de la API de Java.

Cualquier archivo JAR necesario para la operación de tiempo de ejecución de la aplicación Java que no se incluyan con el agente, deben incluirse en el valor de configuración *Vía de acceso de clase para jar externos*.

Aplicación Java de ejemplo generada

Una referencia que describe el código que Agent Builder genera y el código que debe añadir o sustituir para los recursos que desee supervisar.

Al crear un agente con uno o varios orígenes de datos de la API de Java, Agent Builder genera el código fuente de la aplicación Java. El código se genera en el proyecto de agente y sigue la estructura del agente. Debe añadir su propio código Java a la aplicación generada. El código recopila datos para los grupos de atributos muestreados, maneja los sucesos que se deben publicar en los grupos de atributos basados en sucesos, informa de errores si se encuentran problemas y ejecuta tareas. La aplicación generada suministra al agente los datos, pero son datos de muestra, que se deben sustituir por los datos obtenidos de los recursos que se desean supervisar.

Un agente de ejemplo se supone que tiene las características siguientes:

- Código de producto: `K91`
- Clase principal de la API de Java: `agent.client.MainClass`
- Estructura del origen de datos de agente tal como se muestra en la Figura 47 en la página 1367:

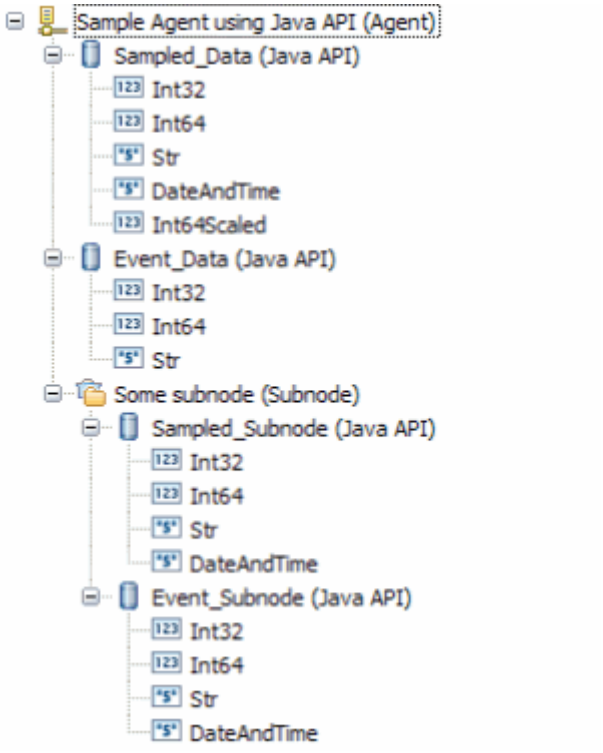


Figura 47. Estructura de agente de muestra

- Propiedad de configuración de *algunos subnodos*: `K91_INSTANCE_KEY`

Estructura de clases

La aplicación Java generada separa, en un grado alto, código que interactúa con el agente de código que interactúa con los recursos que está supervisando. Contiene archivos que modifica y los archivos que no modifica.

Las clases de Java siguientes se crean mediante Agent Builder:

`MainClass (paquete agent.client)`
La clase especificada en la página **Información de origen de datos de la API de Java global**. Esta clase contiene un método principal y un método que maneja las solicitudes de *actuación*. Esta clase hereda desde la clase del ayudante que se describe a continuación. Debe modificar esta clase para interactuar con los recursos que desea supervisar y las acciones que desea realizar.

`MainClassBase (paquete agent.client)`
Una clase auxiliar que inicializa la conexión con el servidor, registra grupos de atributos y espera solicitudes del servidor. No modifique esta clase.

Clases `Sampled_Data`, `Sampled_Subnode`, `Event_Data` y `Event_Subnode` (`paquete agent.client.attributeGroups`)
Hay una clase para cada grupo de atributos API de Java que maneja las consultas de recopilaciones de datos para el grupo de atributos o genera sucesos para el grupo de atributos. Estas clases heredan desde una de las clases de ayudantes que se describen a continuación. Debe modificar estas clases para recopilar datos de los recursos que desea supervisar.

Clases `Sampled_DataBase`, `Sampled_SubnodeBase`, `Event_DataBase` y `Event_SubnodeBase` (`paquete agent.client.attributeGroups`)
Clases auxiliares, una para cada grupo de atributos de la API de Java, que definen la estructura de los atributos del grupo en una clase interna. No modifique estas clases.

Interfaz `ICustomAttributeGroup` (`paquete agent.client.attributeGroups`)
Una interfaz que define métodos públicos en cada clase de grupo de atributos. No modifique esta interfaz.

Agent Builder nunca sobrescribe las clases que puede modificar. Agent Builder las crea solo si no existen.

Las clases del ayudante y la interfaz se sobrescriben cada vez que se guarda Agent Builder. Cuando modifica y guarda el agente, las clases auxiliares se actualizan para reflejar los cambios estructurales en los grupos de atributos de la API de Java. La interfaz y las clases auxiliares contienen un aviso en la cabecera que le recuerda que no modifique el archivo.

Inicialización y limpieza

El método principal de `MainClass` se llama cuando se inicia el agente. Crea una instancia de `MainClass` y luego entra el método de larga ejecución para recibir y manejar las solicitudes del agente.

La mayor parte del código de inicialización y de limpieza debe añadirse a `MainClass`. En el constructor, añada la inicialización que sea necesaria para crear o acceder a sus recursos. Puede que desee abrir conexiones a recursos remoto, crear manejadores o inicializar estructuras de datos.

Antes de que termine el agente , se llama al método `stopDataCollection`. Si desea cerrar conexiones o limpiar antes de que la aplicación Java finalice, añada ese código al método `stopDataCollection`.

Si la inicialización solo se necesita para un grupo de atributos en particular, la inicialización se puede añadir al constructor de la clase del grupo de atributos. De forma similar, si es necesaria cualquier limpieza para un grupo de atributos en particular, el código de limpieza se puede añadir al método `stopDataCollection` del grupo de atributos.

Cualquier código de la aplicación Java puede utilizar el objeto del programa de registro para grabar entradas de registro. (La clase auxiliar principal crea un objeto de registrador protegido en su constructor. Los objetos auxiliares del grupo de atributos crean una referencia protegida para ese registrador en sus constructores). El objeto del programa de registro utiliza el programa de utilidad del registro de rastreo de Java. Los errores y la información de rastreo detallada se puede obtener desde el registro de rastreo que se crea mediante el programa de registro. La información de rastreo es importante para la resolución de problemas con el proveedor.

Cuando se llama a `stopDataCollection`, si pasa el trabajo de limpieza a otra hebra, espere a que la hebra finalice antes de volver del método `stopDataCollection`. De lo contrario, el trabajo de limpieza se puede terminar abruptamente cuando finaliza el proceso porque la hebra principal se ha completado.

Uno de los valores de configuración del agente es para el nivel de rastreo de Java. La tabla siguiente muestra los valores que puede establecer en la propiedad de configuración JAVA_TRACE_LEVEL. Si la API creó el registrador por usted, la tabla muestra el Nivel utilizado por el registrador.

Tabla 285. Opciones de nivel de rastreo de Java

Nivel de rastreo configurado	**Nivel de rastreo de registro Java**	**Descripción**
Desactivado	APAGADO	No se realiza ningún registro.
Error	GRAVE	Problemas de rastreo que se han producido en la aplicación Java.
Aviso	AVISO	Errores de registro y errores potenciales.
Información	INFORMACIÓN	Rastrear información importante sobre la aplicación Java.
Depuración mínima	BUENO	Rastrear detalles de nivel superior necesarios para analizar el comportamiento de la aplicación Java.
Depuración media	MEJOR	Rastrear detalles acerca del flujo del programa de la aplicación Java.

Tabla 285. Opciones de nivel de rastreo de Java (continuación)		
Nivel de rastreo configurado	**Nivel de rastreo de registro Java**	**Descripción**
Depuración máxima	LA MEJOR	Rastrear todos los detalles sobre la aplicación Java.
Todos	TODOS	Rastrear todos los mensajes.

El nombre del archivo de registro que crea la aplicación Java en este ejemplo es `k91_trace0.log`. Si el agente es un agente de varias instancias, el nombre de la instancia se incluye en el nombre del archivo de registro.

Nota: No grabe mensajes para la salida de error estándar ni para la salida estándar. En sistemas Windows, estos mensajes se pierden. En sistemas UNIX y Linux, estos datos se graban en un archivo que no se recorta.

Recopilación de datos de grupo de atributo de muestra

La clase de un grupo de atributos muestreados (uno que recopila una o varias filas de datos) contiene el método `collectData`, por ejemplo, `Sampled_Data.collectData`. Este método se llama siempre que el agente solicite datos.

La clase auxiliar del grupo de atributos define una clase interna denominada Atributos. Esta clase tiene un campo para cada atributo definido en el grupo de atributos. Los atributos derivados no están incluidos, ya que los calcula el agente. Los tipos de datos de los campos de atributos son equivalentes Java de los tipos de atributos de Tivoli Monitoring, como se muestra en (Tabla 286 en la página 1369).

Tabla 286. Los tipos de datos de los campos de atributos y sus equivalentes tipos de atributos de IBM Tivoli Monitoring	
Tipo de Tivoli Monitoring	**Tipo de datos del campo de atributo**
Serie	Serie
Numérico, de 32 bits, sin ajuste decimal	int
Numérico, de 64 bits, sin ajuste decimal	largo
Numérico, ajuste decimal distinto a cero	doble
Indicación de fecha y hora	Calendario

El método `collectData` debe:

1. Recopilar los datos apropiados del recurso que se supervisa.
2. Crear un objeto Atributos.
3. Añadir los datos a los campos del objeto Atributos.
4. Llame al método `Attributes.setAttributeValues` para copiar los datos en un almacenamiento intermedio interno.
5. Repita los pasos del 1 al 4 según sea necesario para cada fila de datos. (Puede saltarse los pasos del 1 al 4 y no devolver filas. En este caso, la columna Código de error de la tabla Estado de objeto de rendimiento tiene el valor NO_INSTANCES_RETURNED. Para obtener más información sobre códigos de error, consulte “Códigos de error” en la página 1372.
6. Llame a `AgentConnection.sendData`para enviar los datos al agente, o llame a `sendError` para descartar los datos copiados de las llamadas a `setAttributeValues`y envíe un código de error en su lugar.

Debe recopilar los datos del recurso (Paso 1), sustituyendo los datos de muestra utilizados en la aplicación generada.

Para llenar el objeto Atributos, puede pasar los datos utilizando el constructor Atributos (como se hace en la aplicación generada). De forma alternativa, utilice el constructor de argumento cero para crear un objeto Atributos y luego asignar los campos del objeto Atributos a los valores de atributos que ha recopilado. Los campos tienen el mismo nombre que los atributos, aunque empiezan por minúscula.

Recopilación de datos de muestra para un subnodo

Si un grupo de atributos muestreado es un subnodo, probablemente se están supervisando varios recursos (uno diferente para cada subnodo). Debe determinar de qué recurso se debe recopilar datos. Debe haber una o más propiedades de configuración que identifiquen qué recurso se está supervisando.

Para este ejemplo, se supone que una propiedad de configuración, `K91_INSTANCE_KEY`, contiene un valor que identifica el recurso del que se deben recopilar datos.

Efectúe los pasos siguientes para encontrar el recurso correcto:

1. Obtenga el ID de instancia de todos los subnodos configurados llamando a `AgentConnection.getConfiguredSubnodeInstanceIDs`. Cada subnodo que se configura tiene un ID de instancia exclusivo.
2. Para cada ID de instancia, obtenga la propiedad de configuración `K91_INSTANCE_KEY` llamando a `AgentConnection.getSubnodeConfigurationProperty`.
3. Busque el recurso representado por el valor en `K91_INSTANCE_KEY`.

Estos pasos pueden realizarse en el método `collectData` antes de la serie de pasos detallados en (“Recopilación de datos de grupo de atributo de muestra” en la página 1369).

De forma alternativa, puede realizar estos pasos en el constructor de clases de grupos de atributos y establecer una correlación directa desde el ID de instancia con el recurso. Un ejemplo de constructor de clases de grupos de atributos es el constructor `Sampled_Subnode`. Este procedimiento también ofrece la oportunidad de crear manejadores o conexiones abiertas que se pueden utilizar durante la vida del agente. La creación de manejadores o de conexiones abiertas puede hacer que el acceso a recursos sea más eficiente.

El código generado crea objetos de recursos de muestra de tipo `MonitoredEntity` en el constructor, y los añade a una correlación `configurationLookup`. Debe eliminar la clase interna `MonitoredEntity`, y sustituir los objetos `MonitoredEntity` por objetos que accedan a sus propios recursos. Si elige realizar todo el procedimiento de búsqueda en el método `collectData`, puede eliminar la correlación `configurationLookup` de la clase.

Si decide utilizar el constructor, para correlacionar el ID de instancia de subnodo con el recurso, los pasos del método `collectData` son:

1. Recuperar el ID de instancia del subnodo del parámetro de solicitud, llamando a `Request.getSubnodeInstanceID`.
2. Recuperar el objeto de recurso desde la correlación creada en el constructor.
3. Realizar la serie de pasos detallados en “Recopilación de datos de grupo de atributo de muestra” en la página 1369 para enviar datos al agente.

Se elige una propiedad de subnodo arbitraria en el ejemplo de Agent Builder, en este caso `K91_INSTANCE_KEY`. Si no es la propiedad correcta, o si se necesita más de una propiedad para identificar el recurso correcto, debe elegir las propiedades para identificarlo.

Envío de sucesos

Para grupos de atributos que generan sucesos, no hay ninguna llamada periódica a un método `collectData`. Los sucesos se envían por medio de la aplicación como el recurso los envía.

Como ejemplo de producción de sucesos, el código generado para un grupo de atributos basado en sucesos crea e inicia una hebra que se ejecuta desde una clase interna llamada `SampleEventClass`. El grupo de atributos basado en sucesos utilizado en el ejemplo es la clase `Event_Data`. La hebra se despierta periódicamente y envía un suceso. Si desea sondear periódicamente el recurso para los sucesos, puede utilizar la estructura de la clase `Event_Data` como se generó:

1. En el constructor `Event_Data`, cree e inicie una hebra.
2. En el método de ejecución de la hebra, ejecute el bucle hasta que el agente termine.
3. Suspenda durante un periodo de tiempo antes de buscar sucesos. Puede cambiar el intervalo de sondeo de 5000 milisegundos a un número que tenga sentido para el agente.
4. Determine si se ha producido uno o más sucesos. La aplicación generada no lo comprueba, pero siempre publica un único suceso.
5. Para cada suceso que deba publicarse, obtenga los datos del suceso a publicarse.
6. Cree y llene un objeto Atributos (como hizo el método `collectData` para un grupo de atributos muestreados).
7. Llame al método `Attributes.sendEventData`. Los sucesos constan de una única fila, por lo que sólo se puede enviar un único suceso cada vez.

De forma alternativa, si trabaja con una API de Java que informa de sucesos desde su propia hebra, puede inicializar la hebra en el constructor `Event_Data`. También puede registrar su propio objeto de manejo de sucesos en el mecanismo de manejo de sucesos de su recurso. En el manejador de sucesos, siga estos pasos:

1. Obtenga los datos de sucesos que se publicarán.
2. Cree y rellene el objeto Atributos.
3. Llame al método `Attributes.sendEventData`.

En este caso, no tiene por qué crear su propia hebra en la clase `Event_Data` ni tampoco necesita la clase `SampleEventClass`.

Envío de sucesos en un subnodo

Cuando se detecta un suceso para un grupo de atributos de un subnodo, la aplicación Java debe publicar el suceso en el subnodo correcto.

Para este ejemplo, se supone que una propiedad de configuración, `K91_INSTANCE_KEY`, contiene un valor que identifica una instancia de un recurso que puede producir sucesos. También se supone que el valor de la propiedad `K91_INSTANCE_KEY` se recupera junto con los datos que se publicarán en el suceso. Para recuperar la propiedad y los datos, la aplicación de Java sigue estos pasos:

1. Obtiene los datos de sucesos que se publicarán, junto con la “clave de instancia”.
2. Crea y rellena el objeto Atributos.
3. Obtiene una lista de todos los ID de instancias de subnodos configuraciones llamando a `AgentConnection.getConfiguredSubnodeInstanceIDs`.
4. Para cada instancia de subnodo, capta el valor de `K91_INSTANCE_KEY` llamando a `AgentConnection.getSubnodeConfigurationProperty`.
5. Cuando se encuentra el valor de `K91_INSTANCE_KEY` que coincide con el valor obtenido con los datos de suceso, recuerda al ID de instancia del subnodo correspondiente.
6. Llama a `Attributes.sendSubnodeEventData`, pasando el ID de instancia de subnodo recordado.

La aplicación generada no realiza la búsqueda descrita en los pasos 4 y 5, en su lugar publica un suceso en el grupo de atributos de cada subnodo. Probablemente este comportamiento no sea el correcto para un agente de producción.

Mandatos de `actuación`

Los mandatos de `actuación` se definen en Tivoli Enterprise Portal o utilizando el mandato `tacmd createaction`. Las acciones se pueden importar al proyecto de Agent Builder para que se creen cuando se instale el agente. Para obtener más información sobre la importación de mandatos de `actuación`, consulte el “Importación de archivos de soporte de aplicaciones” en la página 1444.

La aplicación Java generada registra las acciones que comienzan con el código de producto del agente, como por ejemplo, `K91Refresh`. Este registro se realiza en la clase auxiliar principal (`MainClassBase`)

desde el método `registerActionPrefix`. Si desea registrar otros prefijos, o no registrar ninguna acción, sustituya `registerActionPrefix` en `MainClassBase`.

Cuando el agente desea ejecutar una acción que empieza con un prefijo registrado por el agente, se llama al método `MainClass.takeAction`. Puede añadir código para llamar a `Request.getAction()`, realizar la acción apropiada y luego llamar a `AgentConnection.sendActionReturnCode` para enviar el código de retorno de la acción. Un código de retorno de `0` significa que la acción es satisfactoria, cualquier otro código de retorno significa que la acción falló.

Manejo de excepciones

Los métodos `collectData` y `takeAction` pueden emitir cualquier excepción de Java, por lo que puede permitir que el código de recopilación emita excepciones sin captarlas. Se llama al método `handleException` (para `collectData`) o al método `handleActionException` (para `takeAction`) cuando la clase auxiliar recibe la excepción.

Para las excepciones de `collectData`, debe llamar a `AgentConnection.sendError` cuando se produce una excepción o cuando hay un problema en la recopilación de datos. La aplicación generada pasa el código de error `GENERAL_ERROR`. Sin embargo, debe sustituir este código de error por uno definido por el agente que mejor describa el problema encontrado. Para obtener más información sobre la adición de códigos de error, consulte el paso "13" en la página 1363.

Para las excepciones de `takeAction`, debe llamar a `AgentConnection.sendActionReturnCode` con un código de retorno no cero.

Algunos métodos de `AgentConnection` emiten excepciones que se derivan de `com.ibm.tivoli.monitoring.agentFactory.customProvider.CpciException`. No se llama al método `handleException` si se emite una `CpciException` durante la recopilación de datos, ya que la clase auxiliar maneja la excepción.

Nota: Si elige captar las excepciones dentro del método `collectData` en lugar de utilizar el método `handleException`, asegúrese de que se vuelven a emitir todas las `CpciException`. Se debe asegurar de que las `CpciException` se vuelven a emitir para que se puedan manejar por la clase base.

Códigos de error

Una respuesta típica a una excepción o a otro error de recurso es enviar un código de error al agente llamando al método `AgentConnection.sendError`. Se puede enviar un error para un grupo de atributos basados en sucesos en cualquier momento. Un error para un grupo de atributos muestreados solo se puede emitir en respuesta a una solicitud de recopilación de datos y en lugar de la llamada a `sendData`.

Si envía un error al agente, tendrá lugar lo siguiente:

1. Se registra un mensaje de error en el registro de rastreo del agente. Este mensaje de error incluye el código de error y el mensaje definido para dicho código de error.
2. Hay una consulta de Estatus de objeto de rendimiento que se puede visualizar para obtener información de estado acerca de los grupos de atributos. La columna Código de error se establece en el tipo Código de error definido para el error que ha enviado. El estado de error se borra una vez que el agente recibe correctamente los datos para el grupo de atributos. Si responde a una solicitud de recopilación de datos con una llamada a `sendData` pero no ha incluido ninguna fila de datos, obtendrá `NO_INSTANCES_RETURNED` en la columna Código de error.

La tabla siguiente describe algunos códigos de error que son internos para el agente que puede esperar ver en ciertas situaciones:

Tabla 287. Códigos de error internos para el agente

Código de error	**Descripción**
`NO_ERROR`	No hay ningún problema en este momento con el grupo de atributos.

Tabla 287. Códigos de error internos para el agente (continuación)	
Código de error	**Descripción**
NO_INSTANCES_RETURNED	La aplicación Java respondió a una solicitud de recopilación de datos, pero no facilitó datos. No proporcionar datos no es un error. Generalmente indica que el grupo de atributos no está supervisando ninguna instancia del recurso.
OBJECT_NOT_FOUND	El agente ha intentado recopilar datos de un grupo de atributos que no se ha registrado a través de la API de cliente. Este error puede significar que la aplicación no ha podido iniciar o no ha iniciado el grupo de atributos cuando el agente ha intentado recopilar datos.
OBJECT_CURRENTLY_UNAVAILABLE	La aplicación envió al agente un código de error que no está definido en la lista global de códigos de error.
GENERAL_ERROR	Se ha producido un problema al recopilar datos de la aplicación, normalmente debido a que la aplicación no respondió a la consulta dentro del intervalo del tiempo de espera. Consulte el registro del rastreo de agente para obtener más detalles. La aplicación también especifica GENERAL_ERROR como código de error, pero es mejor si se define un código de error más detallado.

Cambios en el agente

Determinados cambios en el agente requieren que se realicen los cambios correspondientes en la aplicación Java. Si los cambios estructurales son complejos, puede suprimir cualquiera o todos los archivos de origen de Java antes de guardar el agente. También puede suprimir los archivos si desea volver a iniciar sin las personalizaciones que ha realizado.

La tabla siguiente describe las modificaciones necesarias para los archivos de origen de aplicación Java después de realizar determinados cambios en Agent Builder al guardar el agente.

Tabla 288. Cambios en un agente que requieren modificaciones en el origen Java		
Cambio en el agente	**Qué hace el Agent Builder**	**Cambios manuales necesarios en el origen de Java**
Cambio del nombre del paquete de la clase principal	• Genera todas las clases en la nueva estructura de paquetes. • Elimina todas las clases del ayudante del paquete antiguo.	• Mueva el contenido de las clases de grupo de atributos y principal desde las clases del paquete antiguo a las clases del paquete nuevo. • Elimine las clases del paquete antiguo una vez que la migración se completa.
Cambio del nombre de la clase principal	• Crea nuevas clases principales. • Elimina la antigua clase del ayudante principal.	• Mueva el contenido de clase principal a la nueva clase. • Actualice las referencias al nombre de la clase desde las clases del grupo de atributos.

Tabla 288. Cambios en un agente que requieren modificaciones en el origen Java (continuación)

Cambio en el agente	Qué hace el Agent Builder	Cambios manuales necesarios en el origen de Java
Adición de un grupo de atributos de la API de Java	• Crea clases para el nuevo grupo de atributos. • Añade el registro para el nuevo grupo de atributos en la clase de ayudante principal.	Sobrescriba el código de muestra con la lógica personalizada en la clase del grupo de atributos.
Eliminación de un grupo de atributos de la API de Java	Elimina el registro desde la clase del ayudante principal.	• Elimine la clase de grupo de atributos o mueva la lógica personalizada a alguna otra clase. • Elimine la clase del ayudante del grupo de atributos.
Cambio de nombre de un grupo de atributos de la API de Java	• Crea clases para el nuevo nombre del grupo de atributos. • Actualiza el registro para el grupo de atributos con el nombre cambiado en la clase de ayudante principal.	• Mueva la lógica personalizada de la clase de grupo de atributos con el nombre antiguo a la clase de grupo de atributos con el nombre nuevo. • Elimine la clase del grupo de atributos con el nombre antiguo. • Elimine la clase del ayudante del grupo de atributos con el nombre antiguo.
Adición de un atributo a un grupo de atributos de la API de Java	Actualiza la clase interna de Atributos en la clase del ayudante del grupo de atributos.	Recopile datos para el nuevo atributo en la clase del grupo de atributos.
Eliminación de un atributo desde un grupo de atributos de la API de Java	Actualiza la clase de Atributos en la clase del ayudante del grupo de atributos.	Elimine la recopilación de datos para el atributo anterior en la clase del grupo de atributos.
Cambio del nombre de un atributo en un grupo de atributos de la API de Java	Actualiza el nombre del atributo en la clase Atributos de la clase del ayudante del grupo de atributos.	Actualice cualquier referencia al nombre del atributo en la clase Atributos (con frecuencia no hay referencias debido a que se utiliza el constructor Atributos con argumentos posicionales).
Reordenación de atributos en un grupo de atributos de la API de Java	Actualiza el orden de los atributos en la clase Atributos de la clase del ayudante del grupo de atributos.	Actualice el orden de los argumentos en cualquier llamada al constructor Atributos.

Algunos de los cambios mencionados en la tabla anterior se pueden racionalizar si utiliza la acción Refactorizar - Renombrar de Eclipse. Utilice esta acción en todos los nombres afectados (incluidos los nombres de la clase de ayudante) antes de guardar el agente cambiado.

Utilización de la API de Java

La API de Java se utiliza en todo la aplicación Java generada para comunicarse con el agente. Con frecuencia su única interacción directa con la API de Java es para modificar un parámetro de una llamada

a método existente. Por ejemplo, cambiar un código de error publicado de GENERAL_ERROR a un código de error definido en el agente.

Si desea realizar una codificación más extensiva con la API de Java, puede ver el Javadoc en el editor de texto de Eclipse. Puede ver el Javadoc mientras edita el código Java siguiendo estos pasos:

1. Resalte un nombre de paquete, de clase o de método desde la API.
2. Pulse **F1** para abrir la vista de la ayuda de Eclipse.
3. Seleccione el enlace del Javadoc.

También puede ver una breve descripción desde el Javadoc al pasar el ratón por encima del nombre de una clase o método. El Javadoc de la API se puede encontrar también en el Tivoli Monitoring Knowledge Center, consulte Javadoc.

Las clases para la API de Java se encuentran en `cpci.jar`. El archivo `cpci.jar` se añade automáticamente a la vía de acceso de construcción Java del proyecto al crear un agente que contiene un grupo de atributos de la API de Java. El archivo también se añade al importar un agente que contiene un grupo de atributos de la API de Java. El archivo también se añade al añadir un grupo de atributos de la API de Java a un agente existente. `cpci.jar` también se empaqueta automáticamente con cada agente que contiene un grupo de atributos de la API de Java y se añade a la CLASSPATH de la aplicación Java.

Configuración de la API de Java
Cuando se define un origen de datos de la API de Java en el agente, algunas propiedades de configuración se crean automáticamente.

Si define un origen de datos de la API de Java en el agente, este debe utilizar Java para conectarse al servidor de la API de Java. Las propiedades de configuración de Java se añaden al agente automáticamente. Las siguientes propiedades de configuración de Java son específicas de la configuración del tiempo de ejecución del agente:

Tabla 289. Propiedades de configuración de Java

Nombre	Valores válidos	Necesario	Descripción
Inicio de Java	Vía de acceso completa a un directorio	No	Una vía de acceso completa que apunta al directorio de instalación de Java.
Nivel de rastreo de Java	Opción	Sí	Utilice esta propiedad para especificar el nivel de rastreo utilizado por los proveedores de Java.
Argumentos de JVM	Serie	No	Utilice esta propiedad para especificar una lista opcional de argumentos para la máquina virtual de Java.
Vía de acceso de clases para los jar externos	Serie	No	Vía de acceso que contiene los archivos JAR que no se incluyen con el agente, pero que son necesarios para la operación del cliente de tiempo de ejecución.

Estas variables de configuración están disponibles en la página **Información de configuración de tiempo de ejecución** de Agent Editor bajo **Configuración de la máquina virtual Java (JVM)** y **Configuración de la API de Java**.

Prueba de grupos de atributos de aplicación Java

Puede probar el grupo de atributos de aplicación Java que creo, dentro de Agent Builder.

Antes de empezar

Restricción: A diferencia de la mayoría de los otros grupos de atributos, no puede probar el grupo de atributos de la aplicación Java mientras se crea. Puede probar el grupo de atributos cuando se añade al agente y el agente se guarda. El guardar el agente provoca que se genere el código de Java para el grupo de atributos.

Procedimiento

1. Seleccione un grupo de atributos en la página **Agent Editor Definición de origen de datos** después de la creación del agente y pulse **Probar** .

   Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208

   Después de pulsar **Probar** en uno de los dos pasos anteriores, se visualiza la ventana **Probar cliente de Java**.
2. Opcional: Antes de iniciar la prueba, establezca las variables de entorno, las propiedades de configuración y la información de Java. Para obtener más información, consulte "Prueba de grupo de atributos" en la página 1417. Si desea más información sobre propiedades de configuración predeterminadas para el tiempo de ejecución Java, consulte "Configuración de la API de Java" en la página 1375.
3. Pulse **Iniciar agente**. Una ventana indica que el agente se está iniciando.
4. Para simular una solicitud de Tivoli Enterprise Portal o SOAP para los datos de agente, pulse **Recopilar datos**.

   El agente supervisa el cliente de Java en busca de datos. La ventana **Probar cliente de Java** muestra todos los datos que se devuelven.
5. Opcional: Pulse **Comprobar resultados** si los datos devueltos no son los que esperaba.

   Se abre la ventana **Estado de la recopilación de datos** y muestra más información sobre los datos. Los datos que la ventana Estado de recopilación de datos recopila y muestra, se describen en "Nodo Estatus de objeto de rendimiento" en la página 1462
6. Detenga el agente pulsando **Detener agente**.
7. Pulse **Aceptar** o **Cancelar** para salir de la ventana **Probar cliente de Java**. Al pulsar **Aceptar** se guardan los cambios realizados.

Conceptos relacionados

"Pruebas del agente en Agent Builder" en la página 1417
Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Creación de conjuntos de datos a partir de orígenes existentes

Cuando existe al menos un conjunto de datos, puede crear un conjunto de datos nuevo mediante datos de un conjunto de datos existente.

La opción para crear un conjunto de datos nuevo está disponible en la página **Origen de datos inicial del agente** y en la página **Ubicación de origen de datos**. Puede crear un conjunto de datos utilizando orígenes de datos existentes de las formas siguientes:

1. Mediante la unión de datos de dos conjuntos de datos (grupos de atributos) existentes. Para obtener más información, consulte "Unión de dos grupos de atributos" en la página 1377.
2. Mediante el filtrado de datos de un conjunto de datos (grupo de atributos) existente. Para obtener más información, consulte "Creación de un grupo de atributos filtrado" en la página 1382.

Consejo: La opción para unir dos conjuntos de datos solo está disponible después de que se hayan creado dos o más conjuntos de datos.

Unión de dos grupos de atributos

Cree un grupo de atributos a partir de otros dos grupos de atributos.

Acerca de esta tarea

La unión de grupos de atributos es más útil cuando el agente recopila datos de dos tipos diferentes de orígenes de datos. Por ejemplo, el agente puede recopilar datos WMI y PerfMon, u orígenes de datos SNMP y de script. Cada conjunto de atributos puede ser más útil cuando se utiliza junto con una vista de Tivoli Enterprise Portal.

Por ejemplo, suponga que los grupos de atributos están definidos de la siguiente forma:

```
First_Attribute_Group
    index integer
    trafficRate    integer
    errorCount    integer
```

```
Second_Attribute_Group
    index2    integer
    name string
    traffic string
```

Una definición proporciona contadores (como Perfmon) y la otra proporciona información de identificación. Ningún grupo de atributos le es útil por sí mismo. Sin embargo, si puede combinar ambos grupos de atributos utilizando el índice para hacer coincidir las filas apropiadas de cada uno, dispondrá de un grupo de atributos más útil. Puede utilizar el grupo de atributos combinados para visualizar el nombre, el tipo y las medidas juntos.

Este mismo mecanismo se puede utilizar para añadir etiquetas a la información recopilada mediante grupos de atributos normales. Después, la información se puede correlacionar más fácilmente en un sistema de sucesos cuando se detecta un problema. Por ejemplo, una compañía desea gestionar todos sus servidores recopilando datos comunes y utilizando situaciones comunes para supervisar el estado de los servidores. También le gustaría poder identificar los servidores con más información que le indiquen qué aplicación se está ejecutando en un determinado servidor. Desea tener control sobre los valores utilizados en cada servidor, pero no quiere crear agentes diferentes para cada aplicación. Puede conseguir este control creando un grupo de atributos adicional en su único agente de la manera siguiente:

```
Información_aplicación
    application_type     integer
    application_name    string
    application_group    string
```

Este grupo de atributos se definiría como el grupo de atributos de script que recopila sus valores de la configuración del agente. Puede especificar diferentes valores para cada instancia del agente y utilizar un agente para gestionar todos sus sistemas. Este grupo de atributos se puede unir luego a todos los grupos de atributos de origen en los que se puede necesitar esta información de aplicación. A continuación, la información está disponible en Tivoli Enterprise Portal, situaciones, sucesos y datos almacenados.

Al unir dos grupos de atributos, se crea un tercer grupo de atributos. Este grupo de atributos contiene todos los atributos contenidos dentro de los grupos de atributos de origen.

El resultado de una operación de unión varía en función del número de filas que admite cada grupo de atributos de origen. Si ambos grupos de atributos están definidos para devolver solo una única fila de datos, el grupo de atributos unidos resultante tiene una fila de datos. La única fila contiene todos los atributos de ambos grupos de atributos de origen.

Tabla 290. Grupo de atributos de origen uno (una sola fila)

Atributo1	**Atributo2**	**Atributo3**
16	texto	35

Tabla 291. Grupo de atributos de origen 2 (única fila)			
Atributo4	**Atributo5**	**Atributo6**	**Atributo7**
5001	más datos	56	35

Tabla 292. Unión resultante						
Atributo1	**Atributo2**	**Atributo3**	**Atributo4**	**Atributo5**	**Atributo6**	**Atributo7**
16	texto	35	5001	más datos	56	35

Suponga que un grupo de atributos de origen se define para devolver solo una fila (única fila) mientras que el otro puede devolver más de una fila (varias filas). El grupo de atributos unidos resultante contiene el mismo número de filas que el grupo de atributos de origen de varias filas. Los datos del grupo de atributos de una sola fila se añadirán a cada fila del grupo de atributos de varias filas.

Tabla 293. Grupo de atributos de origen uno (una sola fila)		
Atributo1	**Atributo2**	**Atributo3**
16	texto	35

Tabla 294. Grupo de atributos de origen dos (más de una fila)			
Atributo4	**Atributo5**	**Atributo6**	**Atributo7**
usuario1	vía_acceso1	56	35
usuario2	vía_acceso2	27	54
usuario3	vía_acceso3	44	32

Tabla 295. Unión resultante						
Atributo1	**Atributo2**	**Atributo3**	**Atributo4**	**Atributo5**	**Atributo6**	**Atributo7**
16	texto	35	usuario1	vía_acceso1	56	35
16	texto	35	usuario2	vía_acceso2	27	54
16	texto	35	usuario3	vía_acceso3	44	32

Por último, suponga que ambos grupos de atributos de origen están definidos para devolver más de una fila. Debe identificar un atributo de cada grupo de atributos de origen en los que desea realizar la unión. El grupo de atributos resultante contiene filas de datos donde el valor del atributo del primer grupo de atributos coincide con el valor del atributo del segundo grupo de atributos.

Tabla 296. Grupo de atributos de origen 1 (más de una fila)		
Atributo1	**Atributo2**	**Atributo3**
16	texto	35
27	más texto	54
39	otra cadena	66

Tabla 297. Grupo de atributos de origen 2 (más de una fila)			
Atributo4	**Atributo5**	**Atributo6**	**Atributo7**
usuario1	vía_acceso1	56	35

Tabla 297. Grupo de atributos de origen 2 (más de una fila) (continuación)			
Atributo4	**Atributo5**	**Atributo6**	**Atributo7**
usuario2	vía_acceso2	27	54
usuario3	vía_acceso3	44	32

Tabla 298. Unión resultante (unión de Atributo3 y Atributo7)						
Atributo1	**Atributo2**	**Atributo3**	**Atributo4**	**Atributo5**	**Atributo6**	**Atributo7**
16	texto	35	usuario1	vía_acceso1	56	35
27	más texto	54	usuario2	vía_acceso2	27	54

Con Agent Builder, también puede unir grupos de atributos definidos por el usuario al grupo de atributos Disponibilidad si existen filtros de disponibilidad definidos en el agente. Para obtener más información sobre los datos contenidos en el grupo de atributos de Disponibilidad, consulte ("Nodo de disponibilidad" en la página 1457).

Puede crear este tipo de grupo de atributos accediendo al menú del árbol de orígenes de datos pulsando el botón derecho del ratón y seleccionando **Unir grupos de atributos**.

Procedimiento

1. En la página **Definición de origen de datos**, pulse con el botón derecho del ratón uno de los grupos de atributos que desea unir y seleccione **Unir grupos de atributos**.

   Esta opción sólo está visible si hay, como mínimo, dos grupos de atributos definidos. Tener un filtro de disponibilidad definido cuenta como tener un grupo de atributos definido.

   Se visualiza la página **Información de grupo de atributos**.

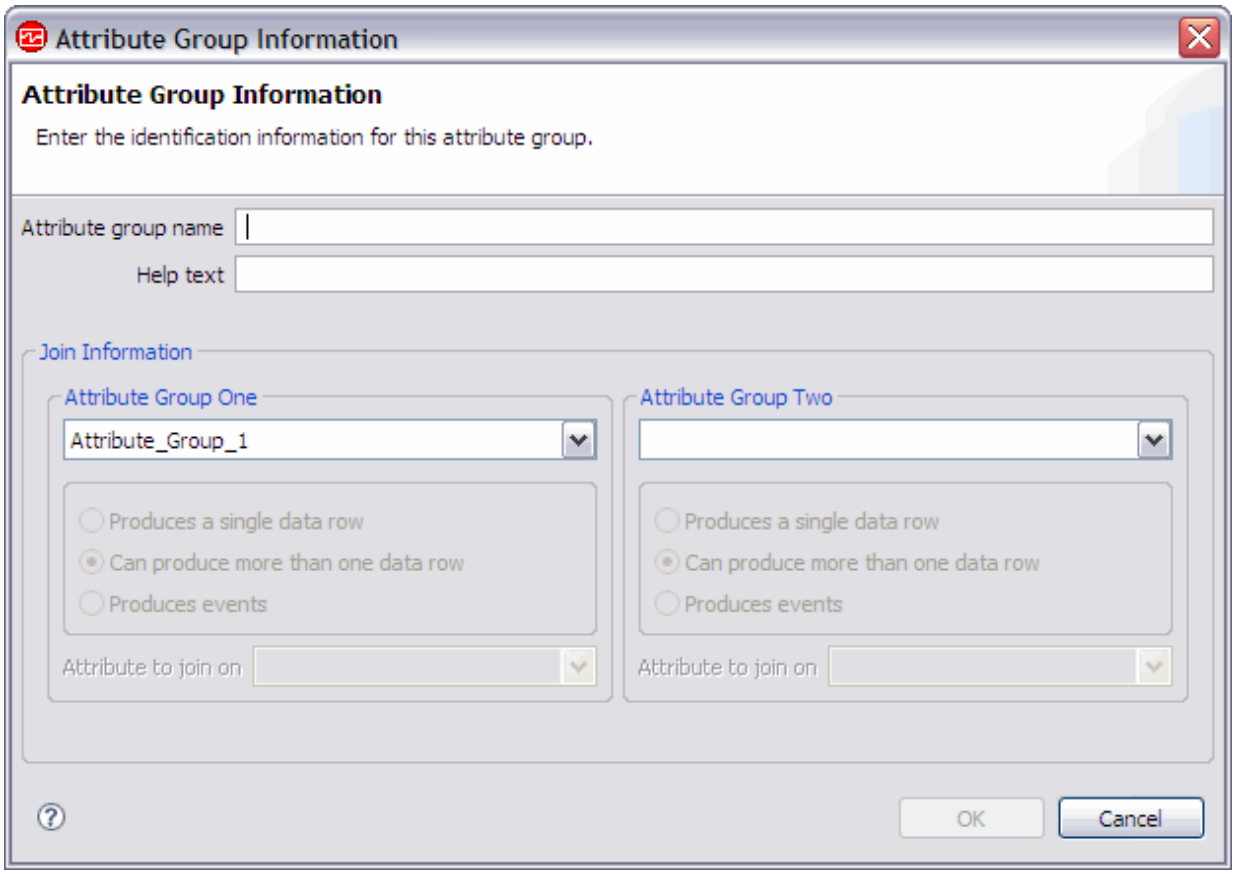


*Figura 48. Página **Información de grupo de atributos** Ventana Información de grupo de atributos*

2. En el área **Información de unión**, seleccione los dos grupos de atributos que desea unir. Seleccione los grupos de atributos realizando la selección en los grupos disponibles en las listas **Grupo de atributos uno** y **Grupo de atributos dos**.

   Para cada grupo de atributos, **Produce una única fila de datos** o **Puede producir más de una fila de datos** se ha seleccionado automáticamente. Esta selección está bloqueada y depende de cómo se han definido originalmente los grupos de atributos de origen.

   Nota: Existen restricciones sobre los grupos de atributos que pueden unirse:

   - No se puede unir un grupo de atributos en un tipo de subnodo a un grupo de atributos en otro tipo de subnodo.
   - Solo puede unir un grupo de atributos de sucesos a un único grupo de atributos de no sucesos.

   a) Seleccione el atributo que desea unirse para cada grupo de atributos cuando ambos grupos de atributos muestran **Puede producir más de una fila de datos**, en **Atributo para unirse**.

   Los campos **Nombre de grupo de atributos** y **Ayuda** se llenan utilizando información de los grupos de atributos elegidos. Si lo desea, puede cambiar estas entradas.
3. Pulse **Aceptar**.

Resultados
El grupo de atributos unido que creó se añade al área **Información de grupo de atributos** de la página **Definición de origen de datos**

Manipulación de atributos en grupos de atributos unidos

La utilización de atributos en grupos de atributos unidos puede imponer reglas sobre cómo se manipulan esos atributos.

Supresión de un grupo de atributos

Un grupo de atributos no se puede suprimir si se hace referencia al mismo en un grupo de atributos de unión a menos que el grupo de atributos unido también se esté suprimiendo.

Supresión de un atributo

No se puede suprimir un atributo si se hace referencia a su grupo de atributos padre en un grupo de atributos unido y una de las siguientes sentencias es verdadera:

- El atributo está definido como atributo de unión en el grupo de atributos unido.
- El atributo se utiliza en cualquier atributo derivado del grupo de atributos unido.

Los atributos unidos no se pueden suprimir. Solos los atributos derivados, si se ha añadido alguno, se pueden suprimir del grupo de atributos unidos.

Reordenación de atributos

El orden de los atributos unidos se fija mediante el orden de los atributos de origen. La lista de atributos unidos no se puede reordenar. Sólo los atributos derivados, si existen, se pueden reordenar.

Cuando la versión de un agente se confirma, los atributos de origen y derivados no se pueden reordenar ni eliminar. Los atributos añadidos en una nueva versión del agente, ya sean atributos de origen o derivados, vendrán después de todos los atributos confirmados. Para obtener más información, consulte “Confirmación de una versión del agente” en la página 1227.

Adición de un atributo

Los nuevos atributos unidos no se pueden añadir de manera explícita. Sólo se pueden crear explícitamente los atributos derivados.

Eliminación de filtros de disponibilidad

El último filtro de disponibilidad no se puede eliminar si se hace referencia al grupo de atributos Disponibilidad en un grupo de atributos unido.

Atributos unidos

Manipule la información relacionada con atributos unidos

Procedimiento

- El nombre de atributo y el texto de ayuda del atributo unido se pueden cambiar para que sean diferentes del atributo de origen:
  a) Seleccione el atributo en el grupo de atributos unidos en el panel **Información de grupo de atributos** de la página **Definición de origen de datos**.
  b) Entre el nuevo nombre y el texto de ayuda.
- El atributo unido se puede mostrar o no en Tivoli Enterprise Portal seleccionando o borrando el recuadro de selección **Visualizar atributo en Tivoli Enterprise Portal**. El recuadro de selección está en la sección **Información de atributo unido** de la página **Definición de origen de datos**. Esta opción es independiente de si el atributo de origen se muestra en Tivoli(r) Enterprise Portal.
- Cualquier atributo o combinación de atributos (que se muestran en Tivoli Enterprise Portal) se pueden marcar con atributos clave marcando el recuadro de selección **Atributo clave**. Esta opción es independiente de si los atributos son atributos clave en los grupos de atributos de origen. La opción también es independiente de si los atributos de origen se muestran en Tivoli(r) Enterprise Portal.
- La información de tipo de atributo para atributos unidos se toma de los atributos de origen y no se puede cambiar en el atributo unido. En la sección **Información de grupo de atributos unidos** del editor de agentes (Figura 49 en la página 1381), pulse **Localizar atributo de origen** para ir al atributo de origen.

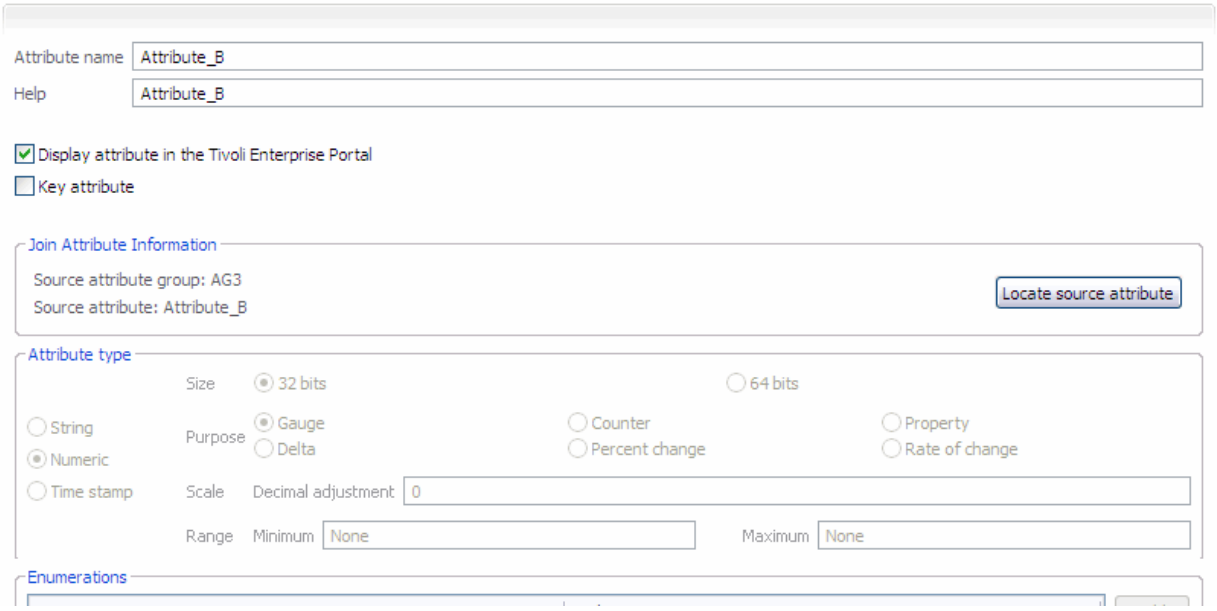


Figura 49. Búsqueda de la información de atributos de origen

Cualquier cambio en los grupos de atributos de origen se refleja en los atributos unidos. Si los grupos de atributos de origen cambian, esos atributos se actualizan automáticamente en el grupo de atributos unidos. Esta actualización automática también se produce si un grupo de atributos diferente se establece como grupo de atributos de origen. Los cambios en un tipo de atributo de origen se copian en el atributo unido. Los cambios en un nombre de atributo de origen o texto de ayuda se copian en el atributo unido. Sin embargo, los cambios de atributo de origen no se copian después de cambiar el nombre o el texto de ayuda de un atributo unido.

Creación de un grupo de atributos filtrado

Cree un grupo de atributos filtrado (conjunto de datos) filtrando las filas de datos de un grupo de atributos existente. Si un conjunto de datos existente devuelve varias filas, puede crear un grupo filtrado devolviendo una fila para utilizarla con IBM Cloud Application Performance Management.

Acerca de esta tarea

Un grupo de atributos filtrado tiene las mismas columnas que el grupo de atributos de origen, pero puede excluir algunas de las filas. Utiliza una fórmula de selección para determinar qué filas se van a incluir.

Para proporcionar información de estado y de resumen para Cloud APM, debe utilizar un conjunto de datos que devuelva una sola fila. Si desea obtener más información al respecto, consulte “Preparación del agente para Cloud APM” en la página 1414. Si la información de origen está en un conjunto de datos que devuelve varias filas, puede crear un grupo de atributos filtrado que devuelve una sola fila.

Por ejemplo, los orígenes de datos del proceso, servicio Windows y código de retorno de mandato proporcionan información como filas en el único conjunto de datos de Disponibilidad. Puede crear un grupo de atributos filtrado, utilizando el campo NAME en la fórmula de selección. El grupo incluye el estado para la aplicación necesaria. Defina que devuelve una fila. A continuación, puede utilizar este grupo de atributos como el conjunto de datos de resumen para Cloud APM.

Un grupo de atributos filtrado resulta también útil cuando una consulta de origen de datos base devuelve datos que prefiere dividir en grupos separados. Windows Performance Monitor, SNMP y WMI son ejemplos de estos orígenes de datos.

Por ejemplo, suponga que un origen de datos puede devolver los datos siguientes:

```
Nombre  Tipo  Tamaño  Utilizado  Libre
Memoria MEM      8     4     4
Disco1  DISK   300   200   100
Disco2  DISK   500   100   400
```

Esta tabla indica el almacenamiento que existe en el sistema e incluye tanto el espacio en memoria como en disco. Puede que prefiera dividir la tabla en memoria y disco como tablas separadas. Puede dividir la tabla creando dos grupos de atributos base. Cada grupo de atributos base recopila los mismos datos y filtra las filas que no desea. Sin embargo, ese no es el método más eficiente para hacer las cosas. En cambio, puede definir un grupo de atributos base que devuelva los datos de uso de disco y memoria juntos. A continuación, defina dos grupos de atributos filtrados. Cada uno utiliza la misma tabla base que su origen. Uno incluye un filtro en el que `Tipo=="MEM"` y el otro incluye un filtro en el que `Tipo=="DISK"`.

En el ejemplo, para el grupo de atributos filtrado donde `Type=="MEM"`, los datos devueltos son:

```
Nombre  Tipo  Tamaño  Utilizado  Libre
Memoria MEM      8     4     4
```

y donde `Type=="DISK"`, los datos devueltos son:

```
Nombre  Tipo  Tamaño  Utilizado  Libre
Disco1  DISK   300   200   100
Disco2  DISK   500   100   400
```

Nota: Los grupos de atributos cuyos datos se basan en sucesos no se pueden utilizar para crear grupos de atributos filtrados. Sólo pueden utilizarse los grupos de atributos cuyos datos están muestreados.

Procedimiento

1. Pulse **Orígenes de datos existentes** en el área **Categorías de datos de supervisión** en la página **Origen de datos inicial del agente** o la página **Ubicación de origen de datos**

   Nota:

   - Se alcanza la página **Origen de datos inicial de agente** utilizando el Asistente de agente nuevo. Para obtener más información, consulte “Crear un agente” en la página 1205.

- Para ir a la página **Ubicación de origen de datos**, pulse con el botón derecho del ratón en un agente en la página **Definición de origen de datos** de **Agent Editor** y seleccione **Añadir origen de datos**.

2. Seleccione **Filtrar filas de datos de un grupo de atributos** en el área **Orígenes de datos**.
3. Pulse **Siguiente**

   Se visualiza la página **Información de filtro**.
4. Seleccione un **Grupo de atributos de origen** en la lista.
5. Especifique la **Fórmula de selección** para filtrar los datos del grupo de atributos que ha seleccionado. Por ejemplo, en la página **Información de filtro** mostrada anteriormente, la fórmula de selección filtra las filas de datos donde el atributo `Tipo` es igual a `"DISK"`. Las filas de datos cuyo atributo `Tipo` no coincide con `"DISK"` se descartan. La fórmula de selección que especifique debe evaluarse a un resultado booleano, true o false.

   Nota: En la página **Información de filtro**, puede pulsar **Editar** para especificar o modificar la fórmula utilizando el Editor de fórmulas. Si desea más información sobre el editor de fórmulas, consulte “Editor de fórmulas” en la página 1239.
6. Pulse **Siguiente**.
7. Seleccione **Produce una única fila de datos** o **Puede producir más de una fila de datos**.
   a) Si ha seleccionado **Puede producir más de una fila de datos**, seleccione un atributo o atributos de clave en la lista.
8. Pulse **Finalizar**.

Creación de un grupo de Navigator

En un entorno IBM Tivoli Monitoring, utilice los grupos de Navigator para agrupar varios orígenes de datos relacionados (grupos de atributos) juntos para que se puedan crear espacios de trabajo que muestren vistas que combinen los orígenes de datos. Puede crear un grupo de Navigator mientras crea un agente utilizando el asistente para agente nuevo en el nivel de agente base. También puede crear un grupo de Navigator al definir un subnodo utilizando el asistente para componente de agente nuevo.

Acerca de esta tarea

Por ejemplo, podría ser capaz de recopilar datos del sistema de archivos de más de un origen de datos. Puede ser útil crear un espacio de trabajo que muestre vistas de todos los datos del sistema de archivos de estos orígenes de datos diferentes.

Los grupos de Navigator también representan una buena forma de ocultar orígenes de datos en el Tivoli Enterprise Portal. Podría decidir que las métricas recopiladas de dos orígenes de datos son más útiles si los orígenes de datos se unen para crear un nuevo origen de datos combinado. Desea ver solo los datos combinados en el origen de datos unido. Puede crear un grupo de Navigator que contenga los tres orígenes de datos y crear un espacio de trabajo que contenga vistas para visualizar únicamente el origen de datos combinado. Los dos orígenes de datos originales están efectivamente ocultos en la vista en Tivoli Enterprise Portal. Consulte el “Creación de conjuntos de datos a partir de orígenes existentes” en la página 1376 para obtener información sobre la unión de orígenes de datos.

Nota: Cuando se agrupan orígenes de datos en un grupo de Navigator, Tivoli Monitoring no asocia ninguna consulta con el grupo de Navigator. Se supone que se define un espacio de trabajo predeterminado para que el grupo de Navigator visualice los orígenes de datos en un formato útil.

Se puede definir un grupo de Navigator en el agente básico o en un subnodo. Un grupo de Navigator no puede contener otro grupo de Navigator.

Los grupos de Navigator no tienen ningún efecto en un entorno IBM Cloud Application Performance Management.

Procedimiento

1. Realice uno de los pasos siguientes:

- Al crear un nuevo agente utilizando el asistente **Agente**, en la página **Origen de datos inicial del agente**, pulse **Agrupaciones de orígenes de datos** en el área **Categorías de datos de supervisión**.
- Con un agente existente, siga los pasos siguientes en Agent Editor:
  a. Pulse el separador **Orígenes de datos** para abrir la página **Definición de origen de datos**.
  b. Seleccione el agente y pulse **Añadir a seleccionados**.
  c. En la página **Ubicación de origen de datos**, en el área **Categorías de datos de supervisión**, pulse **Agrupaciones de orígenes de datos**.

2. En el área **Orígenes de datos**, pulse **Un grupo de Navigator**.
3. Pulse **Siguiente**.
4. En la página **Información de grupo de Navigator**, escriba el nombre del grupo de Navigator y el texto para la Ayuda que desea asociar al nombre, y pulse **Siguiente**.

   Nota: Agent Builder crea automáticamente grupos de Navigator en determinadas situaciones. El siguiente nombre de grupo de Navigator está reservado:

   - Disponibilidad

   .
5. En la página **Origen de datos del primer grupo de Navigator**, seleccione el primer origen de datos de supervisión para el nuevo grupo de Navigator. Pulse una categoría en la lista **Categorías de datos de supervisión** y un origen de datos en la lista **Orígenes de datos**. A continuación, pulse en **Siguiente**.

   Consejo: Puede crear el origen de datos de la forma habitual. Como alternativa, pulse **Orígenes de datos existentes** y elija mover uno o más orígenes de datos que ya haya creado al grupo de Navigator.
6. Si desea crear un origen de datos en un grupo de Navigator, en la página **Definición de origen de datos**, seleccione el grupo de Navigator y pulse **Añadir a seleccionados**.
7. Si desea mover orígenes de datos existentes al grupo de Navigator, en la página **Definición de origen de datos**, seleccione el grupo de Navigator y pulse **Añadir a seleccionados** y en la página **Origen de datos del grupo de Navigator**, seleccione **Orígenes de datos existentes**. En la página **Orígenes de datos definidos actualmente**, seleccione los orígenes de datos.
8. Si desea eliminar un origen de datos de un grupo de Navigator, siga uno de estos pasos en la página de **Definición de origen de datos**:
   - Seleccione el origen de datos y arrástrelo a la raíz del árbol de orígenes de datos.
   - Seleccione el origen de datos y pulse **Eliminar**.
9. Si desea crear un grupo de Navigator, siga uno de los pasos siguientes en la página **Definición de origen de datos**:
   - Pulse en **Añadir al agente**.
   - Seleccione un subnodo y pulse **Añadir a seleccionados**.

Utilización de subnodos

Un subnodo puede usarse para supervisar varios componentes de aplicación desde una única instancia de agente.

Puede crear un único agente que cumpla las tareas siguientes utilizando subnodos:

- Supervisa cada instancia de un servidor de software que se está ejecutando en un sistema, en lugar de tener que utilizar instancias separadas del agente, una por cada instancia del servidor de software.
- Supervisa varios sistemas remotos diferentes en lugar de tener que utilizar instancias diferentes del agente, una para cada sistema remoto.
- Supervisa distintos tipos de recursos desde un agente, en lugar de tener que crear y desplegar varios agentes distintos.

- En IBM Tivoli Monitoring, muestra un nivel adicional en el árbol de navegación físico de Tivoli Enterprise Portal que permite seguir agrupando y personalizando. Además, pueden definirse grupos de sistema gestionado con otro nivel de granularidad en las situaciones.
- En IBM Cloud Application Performance Management, proporciona varios recursos diferentes, visualizando diferentes paneles de instrumentos de resumen y detalle. Los recursos de subnodo pueden mostrarse como iguales o subcomponentes del recurso de agente. Puede incluir estos recursos en aplicaciones de forma independiente.

Pueden crearse tipos de subnodo en Agent Builder. Cada tipo debe corresponder a un tipo distinto de recurso que puede supervisar un agente. Añada orígenes de datos y conjuntos de datos al tipo de subnodo de un determinado recurso supervisado.

Al desplegar el agente en un host supervisado y configurarlo, pueden crearse una o más instancias de cada tipo de subnodo. Cada instancia de un subnodo debe corresponder a una instancia de un servidor, un sistema remoto, o cualquier recurso para el cual el tipo de subnodo ha sido designado para supervisar. Todas las instancias de subnodo de un único tipo de subnodo contienen grupos de atributos y espacios de trabajo que tienen formato idéntico. Sin embargo, cada instancia de subnodo tiene datos que proceden del recurso particular que se está supervisando.

Cuando se configura el agente en el host supervisado, puede determinarse el número de instancias de subnodo. Algunos datos de configuración se pueden aplicar al agente de forma global, pero otros datos de configuración se aplican a una única instancia de subnodo. Configure cada instancia de subnodo de forma diferente a las otras instancias de subnodo, de forma que no supervisen el mismo recurso exacto ni muestren los mismos datos exactos.

En un entorno IBM Tivoli Monitoring, se visualiza una instancia de subnodo dentro del agente en la vista física de navegación en el Tivoli Enterprise Portal. Los espacios de trabajo muestran los datos que genera una instancia de subnodo y pueden distribuirse situaciones a una o más instancias de un subnodo. Se crea automáticamente una lista de sistemas gestionados que contiene todas las instancias del subnodo, como la Lista de sistemas gestionados que se crea para un agente.

En un entorno de IBM Cloud Application Performance Management, puede visualizar tanto las instancias de agente como de subnodo como recursos supervisados. Cada instancia de subnodo se convierte en un recurso separado. Si desea obtener más información al respecto, consulte “Subnodos en IBM Cloud Application Performance Management” en la página 1390.

Dado que los agentes construidos con Agent Builder crean las instancias de subnodo que se basan en los valores de configuración, dichos subnodos tiene el mismo lapso de vida que el agente. Se continúa realizando una pulsación para el agente, no una pulsación distinta para cada subnodo. Por tanto, usando subnodos puede incrementarse significativamente el escalado potencial del entorno de supervisión. La alternativa es utilizar varias instancias de agente, que pueden limitar la posible escala del entorno IBM Tivoli Monitoring o IBM Cloud Application Performance Management.

La adición o eliminación de un subnodo requiere reconfigurar el agente. Para reconfigurar el agente, hay que pararlo y reiniciarlo, implicando a todos los subnodos. El agente puede definirse como un agente de múltiples instancias; en tal caso, puede iniciarse y pararse una única instancia y dejar las otras instancias en ejecución.

Además de los conjuntos de datos de los subnodos, un agente puede definir los conjuntos de datos a nivel de agente que están ubicados fuera de un subnodo.

En el árbol de Tivoli Enterprise Portal Navigator, se visualiza un tipo de subnodo bajo el nombre de agente y se visualizan instancias de subnodo bajo un tipo de subnodo. Los subnodos se identifican mediante un nombre de sistema gestionado (MSN) igual que los agentes, por ejemplo, `94:Hill.cmn`.

Por ejemplo, en el árbol de Navigator en Figura 50 en la página 1386, **Cuidar nuestros amigos** es un agente con tres recursos (**Abordadores**, **Áreas comunes** y **Cursos de canales**) y dos tipos de subnodos (**Área común** y **Curso de canal**). Dos de estos recursos poseen tipos de subnodos definidos para ellos (**Área común** y **Curso de canal**). Un subnodo no es necesario para el tercer recurso (**Abordador**), que se representa mediante una única fila en una tabla en el nivel de agente básico. El tipo de subnodo de Área común tiene tres instancias de subnodo: `94:Hill:cmn`, `94:Meadow:cmn` y `94:Tree:cmn` que representan tres áreas comunes del canal. El tipo de subnodo de Curso de canal tiene cuatro instancias

de subnodo: `94:system1:run`, `94:system2:run`, `94:system4:run` y `94:system5:run` que representan cuatro cursos de canal.

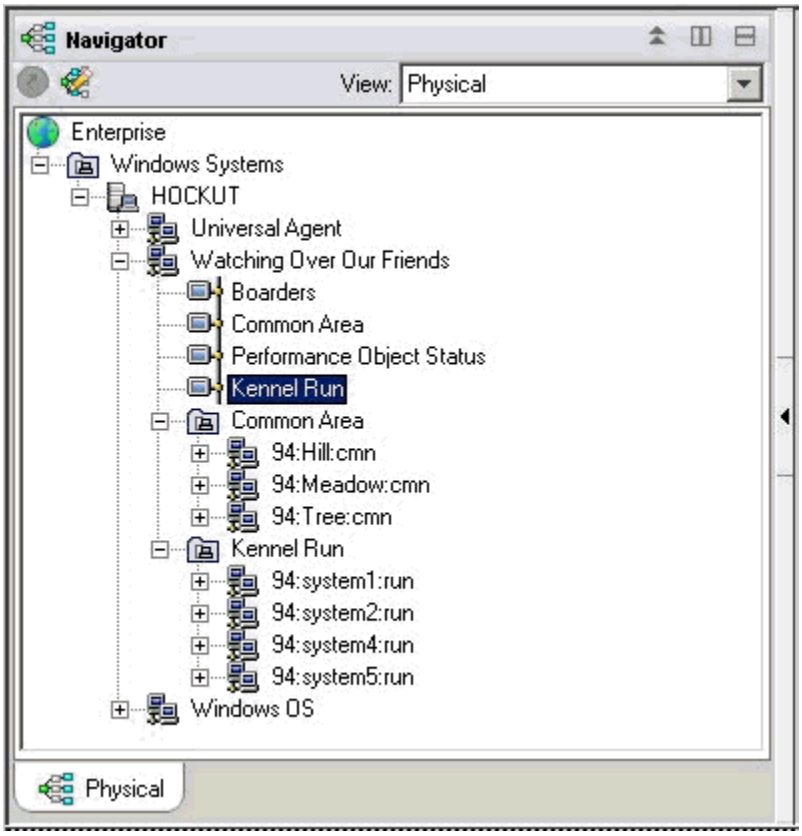


Figura 50. Subnodos del árbol de Navigator

Un agente simple puede utilizar subnodos de dos formas:

- El agente puede tener diferentes subnodos del mismo tipo.
- El agente puede tener subnodos de tipos diferentes.

Subnodos para los mismos datos procedentes de orígenes distintos

Pueden usarse subnodos del mismo tipo para representar varias instancias de un tipo de recurso supervisado. Cada subnodo del mismo tipo incluye los mismos grupos de atributos y los valores correctos de la instancia de recursos supervisada concreta. El número de subnodos varía según la configuración del agente. El ejemplo de la Figura 51 en la página 1387 muestra la supervisión de diferentes sistemas.

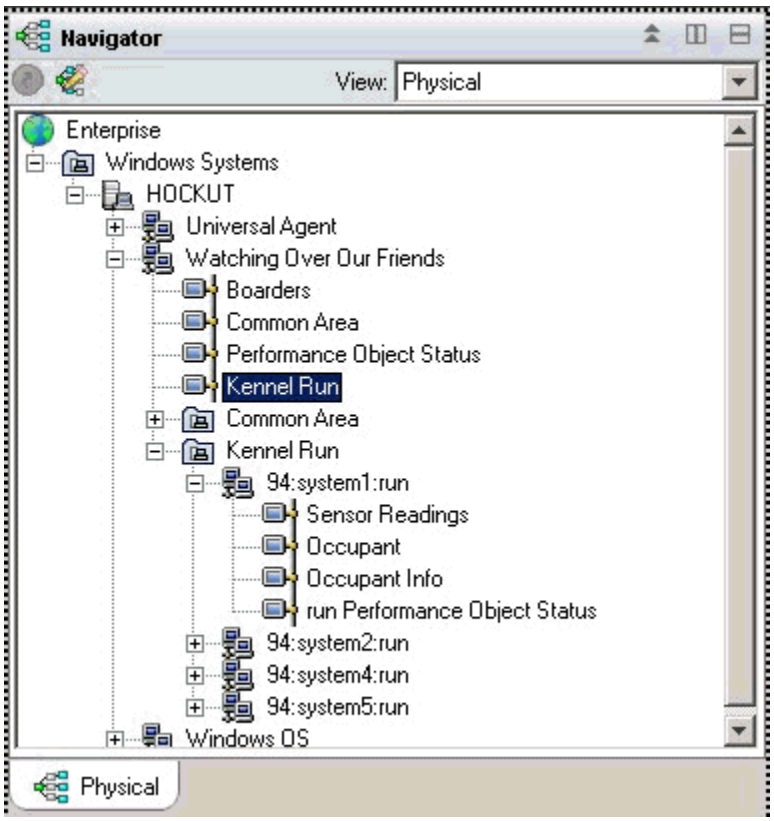


Figura 51. Subnodos que supervisan sistemas diferentes

Subnodos para varios tipos de datos

Cuando un agente supervisa varios tipos de recurso supervisado, puede crearse un tipo de subnodo por cada uno de los tipos de recurso. Cada subnodo incluye la información definida en ese tipo de subnodo. El ejemplo siguiente muestra dos tipos de subnodo. Cada tipo está supervisando un tipo de recurso diferente, con distintos tipos de datos disponibles para cada recurso:

- Área común
- Curso de canal

El agente en Figura 52 en la página 1388 ejecuta una copia de cada tipo de subnodo. Un agente concreto puede crear cualquier subconjunto de agentes definidos. Los subnodos se pueden utilizar para simular perfiles de Tivoli Monitoring V5.

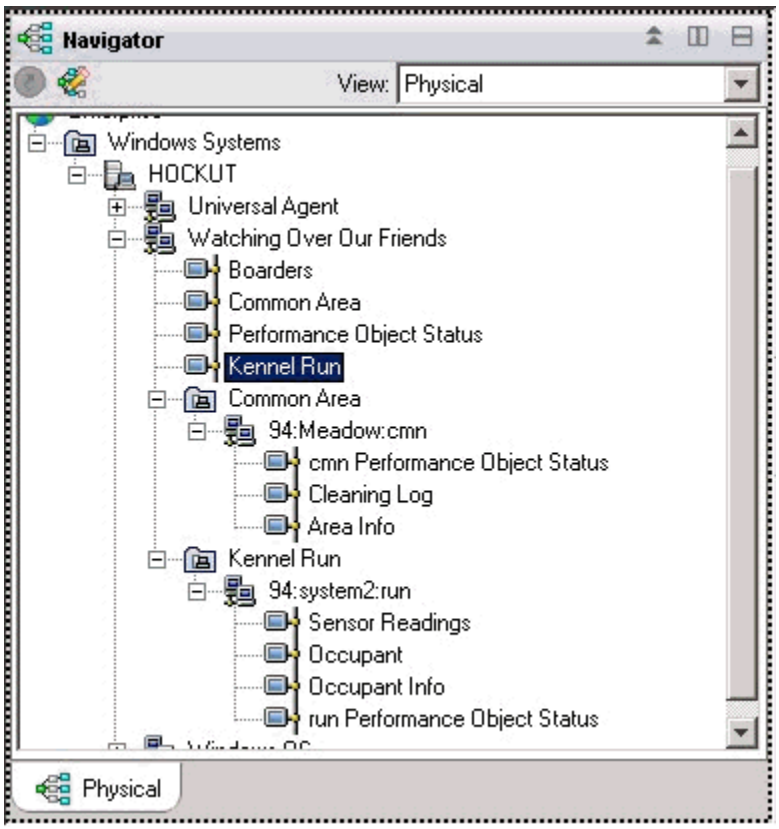


Figura 52. Tipos de subnodo del árbol de Navigator

Ambas formas de utilizar nodos se pueden emplear en el mismo agente, donde cada tipo puede tener más de una instancia de subnodo.

Figura 52 en la página 1388 muestra dos tipos de subnodos que supervisan dos tipos de recursos: áreas comunes y Cursos de canal. Además, hay varios subnodos definidos para cada tipo. Existen tres subnodos de tipo Área común: Pradera, Colina y Árbol. También existen cuatro subnodos de tipo Canal (cada uno recopila datos de un sistema distinto que está dedicado a un Curso de canal); estos subnodos poseen los siguientes ID: sistema1, sistema2, sistema4 y sistema5.

Nota: Los primeros 24 caracteres de ID de subnodo deben ser exclusivos para todas las instancias del tipo de subnodo en la instalación de IBM Tivoli Monitoring.

Proveedores de datos en subnodos

Un subnodo puede contener cualquier combinación de datos de diferentes tipos de proveedores de datos. La mayoría de los proveedores de datos de Agent Builder se pueden utilizar en un subnodo, incluyendo los siguientes proveedores de datos:

- WMI
- Perfmon
- Registro de sucesos de Windows
- SNMP
- Sucesos de SNMP
- JMX
- Ping de ICMP
- Script
- Registro

- CIM
- JDBC
- HTTP
- SOAP
- Socket
- API de Java

Un subnodo también puede contener un grupo de atributos unido que combine datos de dos grupos de atributos distintos del mismo subnodo o de grupos de atributos de nivel de agente.

Estatus de subnodos

Existen dos formas de determinar el estatus para un agente de subnodo. La primer manera es visualizar los datos que se muestran en el grupo de atributos de Estado de objeto de rendimiento. Este grupo de atributos muestra el estatus de cada uno de los grupos de atributos del mismo nivel en el agente. El grupo de atributos Estatus de objeto de rendimiento en el nivel de agente visualiza el estatus de recopilación para los demás grupos de atributos en el nivel de agente. El grupo de atributos Estatus de objeto de rendimiento en cada subnodo muestra el estatus de recopilación para los grupos de atributos en dicho subnodo.

Agent Builder también crea un grupo de atributos por cada tipo de subnodo, que muestra una fila por cada subnodo configurado de dicho tipo. En el ejemplo de la Figura 53 en la página 1389, se ejecutan cuatro subnodos para recopilar datos.

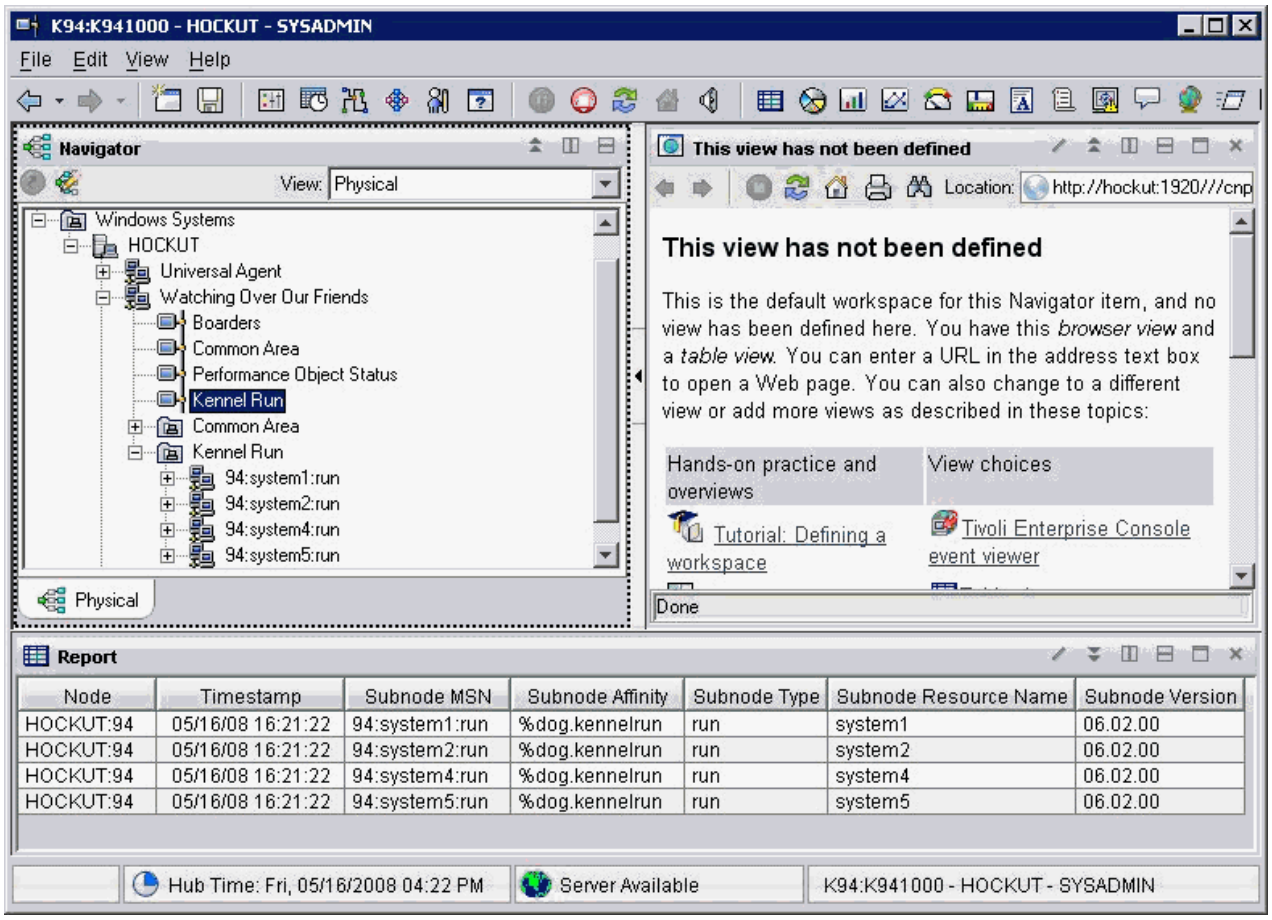


Figura 53. Supervisión de varias instancias de subnodo del mismo tipo de subnodo

En el entorno de IBM Tivoli Monitoring, el subnodo **Estado del objeto de rendimiento** contiene datos visibles en el árbol de Navigator y puede tener situaciones que supervisen el estado de las otras recopilaciones de datos.

En el entorno de IBM Cloud Application Performance Management, puede crear umbrales para supervisar los datos de **Estado del objeto de rendimiento**.

El ejemplo de Figura 54 en la página 1390 muestra un caso en el que la recopilación de datos ha fallado (no se ha encontrado el comando de shell script). Por lo general, cualquier valor que no sea NO_ERROR indica que existe un problema. Para cada uno de los recopiladores de datos que se definen en el subnodo, hay una fila en la tabla.

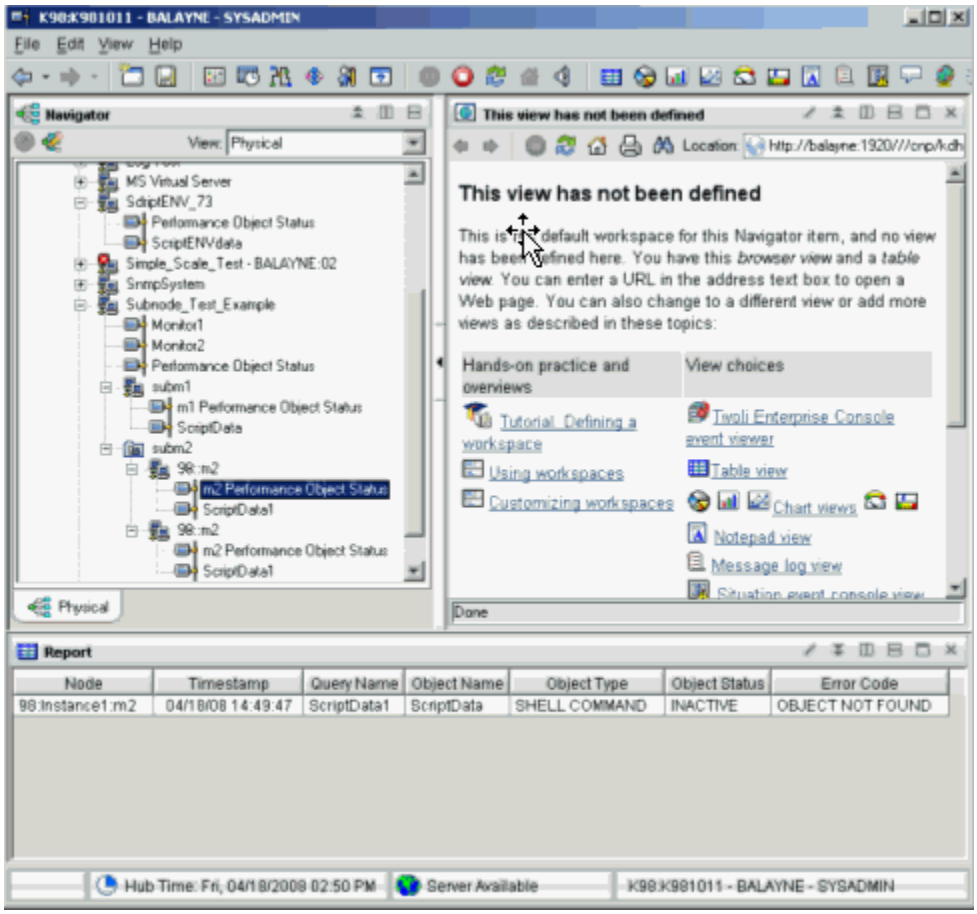


Figura 54. Ejemplo: recopilación de datos en un subnodo

Subnodos en IBM Cloud Application Performance Management

En IBM Cloud Application Performance Management, puede definir la instancia de agente o una instancia de subnodo, o ambas, como recursos supervisados, y cada recurso corresponde a un panel de instrumentos de resumen.

Los paneles de instrumentos de subnodo no pueden mostrar datos de nivel de agente. Para mostrar los datos del nivel de agente en este entorno, defina la un panel de instrumentos de resumen para el agente.

En función de los valores que seleccione, los recursos de agente y subnodo pueden aparecer en el mismo nivel, sin ninguna distinción jerárquica, o los recursos de subnodo pueden aparecer como hijos de recursos de agente.

Para obtener instrucciones sobre cómo configurar recursos de agente y subnodo, consulte “Preparación del agente para Cloud APM” en la página 1414.

Creación de subnodos

Puede crear un subnodo al crear o editar un agente.

Procedimiento

1. Realice uno de los pasos siguientes:
   - Al crear un nuevo agente mediante el **Asistente de agente**, en la página **Origen de datos inicial de agente**, pulse **Agrupaciones de orígenes de datos** en el área **Categorías de datos de supervisión**.
   - Con un agente existente, realice los pasos siguientes en el editor del agente:
     a. Pulse la pestaña **Orígenes de datos** para abrir la página **Definición de origen de datos**.
     b. Seleccione el agente y pulse **Añadir a seleccionados**.
     c. En la página **Ubicación de origen de datos**, en el área **Categorías de datos de supervisión**, pulse **Agrupaciones de orígenes de datos**.
2. En el área **Orígenes de datos**, pulse **Una definición de subnodo**
3. Pulse **Siguiente**.
4. Complete la página **Información de subnodo** como se indica a continuación para definir el nuevo subnodo:
   a) En el campo **Nombre**, escriba el nombre del subnodo que está creando.
   b) En el campo **Tipo**, ingrese de 1 a 3 caracteres (números, letras o ambos) para identificar el tipo de subnodo que está creando.
   c) En el campo **Descripción**, escriba una descripción para el subnodo que está creando.
   d) Pulse el recuadro de selección **Mostrar grupo de atributos de nodos para este tipo de subnodo** para ocultar o mostrar el grupo de atributos de disponibilidad. Para obtener más información sobre este grupo de atributos, consulte "Nodo de disponibilidad" en la página 1457.
   e) Pulse **Siguiente**.
5. Complete la página **Origen de datos del subnodo inicial** para seleccionar un origen de datos como el primer elemento del subnodo nuevo. Pulse una categoría en la lista **Categorías de datos de supervisión** y un origen de datos en la lista **Orígenes de datos**. A continuación, pulse en **Siguiente**.

   Consejo: Puede crear el origen de datos de la forma habitual. De forma alternativa, puede mover uno o varios orígenes de datos que ya ha creado al grupo del navegador. Para mover los orígenes de datos, pulse **Orígenes de datos existentes** y, en la página **Orígenes de datos definidos actualmente**, seleccione los orígenes de datos.

   Importante: No se pueden incluir orígenes de datos de proceso, servicio Windows, o de código de retorno de mandato en un subnodo. Como método alternativo, puede escribir un script que determine el la información de servicio o proceso necesaria y utilizar un origen de datos de salida de script.
6. Si el agente contiene propiedades de configuración personalizadas o si el origen de datos seleccionado necesita configuración, utilice la página **Alteraciones temporales de configuración de subnodo** para elegir las propiedades de configuración.

   En la página **Alteración temporal de configuración de subnodo**, seleccione las propiedades de configuración que desea para el subnodo en el nivel de agente. Después, seleccione las propiedades de configuración que desea variar en cada subnodo.

   Utilice **Mover**, **Copiar** y **Eliminar** para especificar las propiedades de configuración tal como se describe en "Configuración de un subnodo" en la página 1392.
7. Pulse **Siguiente**.

   Se visualiza la página **Definición de origen de datos**.

Configuración del subnodo

Cuando se define un tipo de subnodo, se define una sola sección de configuración específicamente para este subnodo.

Una sección de configuración de subnodo difiere de otras secciones de configuración de varias formas:

- El conjunto de propiedades de una sección de subnodo se puede duplicar, por lo que existen varios conjuntos de propiedades. Cada conjunto de propiedades forma su propia sección. El diseño de todas las secciones es idéntico, pero se pueden entrar valores diferentes en cada sección.

  Por el contrario, las propiedades en otras secciones (a las que se hace referencia como secciones de nivel de agente) se muestran solo durante la configuración de tiempo de ejecución. No forman subsecciones y no se pueden ni duplicar ni eliminar.

  Consulte "Ejemplo de configuración de subnodo" en la página 1395 para ver ejemplos de configuración de subnodos mediante GUI y línea de mandatos.
- Para cada copia de una sección de subnodo que se crea durante la configuración de tiempo de ejecución, el agente crea una instancia de subnodo diferente. Todas estas instancias de subnodo son del mismo tipo.
- Los nombres de propiedades de las secciones de subnodo pueden ser duplicados de nombres de propiedades de secciones del nivel de agente. Cuando se producen nombres duplicados, el valor de propiedad de subnodo sustituye al valor de propiedad del nivel de agente.
- En IBM Tivoli Monitoring V6.2.1 y posteriores, una sección de subnodo puede tener valores de propiedades predeterminados que se apliquen a todas las instancias de subnodos de dicho tipo. Esta característica hace que sea posible tener una búsqueda de tres niveles de un solo valor de propiedad, como se muestra a continuación:
  1. El agente obtiene el valor de propiedad de la subsección de instancia de subnodo.
  2. Si no hay ningún valor configurado en el nivel de instancia de subnodo, el valor de propiedad se obtiene del nivel predeterminado del subnodo.
  3. Si no hay ningún valor configurado en ninguno de los dos niveles, el valor de propiedad se obtiene de una sección de nivel de agente.

Consulte "Ejemplo de configuración de subnodo" en la página 1395 para ver ejemplos de configuración de subnodos mediante GUI y línea de mandatos.

Configuración de un subnodo
Utilice la página **Alteraciones temporales de configuración de subnodo** para configurar un origen de datos de subnodo.

Antes de empezar

Siga los pasos de "Creación de subnodos" en la página 1390 para crear un subnodo.

Acerca de esta tarea

Cuando añade un origen de datos a un subnodo, se presenta la página **Alteraciones temporales de configuración de subnodo** si el origen de datos requiere configuración. Muestra propiedades de configuración personalizadas y cualquier otra propiedad de configuración que se pueda aplicar al tipo de subnodo.

Procedimiento

- En la ventana **Alteraciones temporales de configuración de subnodo**, elija las propiedades de configuración que desea para el subnodo en el nivel de agente. Además, seleccione las propiedades de configuración que desee variar en cada subnodo.
- Utilice **Copiar >>** para copiar propiedades de configuración para que residan en el nivel de agente y en el nivel de subnodo.

  El agente busca primero un valor en el nivel de subnodo y, si no encuentra ningún valor, busca en el nivel de agente. Si una propiedad en ambos niveles es una propiedad necesaria, solo es necesaria en el nivel de agente, es opcional en el nivel de subnodo.
- Utilice **Mover >>** para mover propiedades del nivel de agente al nivel de subnodo. **Mover>>** no está disponible para propiedades que son necesarias para un origen de datos de nivel de agente o para un subnodo de un tipo diferente.

- Utilice **Eliminar** para eliminar una de las dos listas. Las propiedades se pueden eliminar solo si se listan en el nivel de agente y en el nivel de subnodo. Esta función no se puede utilizar para eliminar una propiedad por completo.
- Utilice **<< Copiar** para copiar una propiedad del nivel de subnodo al nivel de agente.
- Utilice **<< Mover** para mover una propiedad del nivel de subnodo al nivel de agente.

Qué hacer a continuación

Puede cambiar la configuración para un subnodo existente utilizando Agent Editor.

Alteraciones temporales de la configuración del subnodo
Utilice la alteración temporal de la configuración del subnodo para sustituir temporalmente las propiedades de configuración del agente por propiedades específicas del subnodo.

El procedimiento en "Configuración de un subnodo" en la página 1392 describe cómo gestionar la configuración del subnodo para propiedades generadas automáticamente. La gestión de propiedades de configuración personalizada es similar. Cualquier propiedad de configuración personalizada que se define, se muestra en la ventana **Alteraciones temporales de configuración de subnodo**.

Cuando copia o mueve una propiedad personalizada desde el nivel del subnodo al nivel de agente, se le solicita la sección en la que desea colocar la propiedad. Puede seleccionar una sección personalizada existente o entrar el nombre de una nueva sección personalizada.

Selección de propiedades de configuración del subnodo

Sin subnodos, todas las instancias de un tipo de origen de datos comparten los parámetros de configuración. Por ejemplo, todos los grupos de atributos de SNMP se conectan al mismo host utilizando el mismo nombre de comunidad. Con subnodos, cada instancia de un subnodo puede conectarse a un host diferente si la propiedad SNMP_HOST se coloca en el nivel de subnodo.

Seleccionar las propiedades que se alterarán temporalmente en el nivel de subnodo es una consideración importante cuando se desarrolla un agente. Si se seleccionan demasiadas propiedades, la sección de configuración de subnodo se vuelve confusa y difícil de gestionar. Si se seleccionan insuficientes propiedades, las funciones del agente pueden estar limitadas cuando alguien desea variar una propiedad de un subnodo al siguiente.

Las propiedades siguientes no se pueden copiar en el nivel de subnodo. (Todos los grupos de atributos de todos los subnodos y del agente básico deben utilizar la misma versión de SNMP y tipo de conexión JMX):

- Versión de SNMP
- Tipo de conexión de servidor MBean JMX
- Directorio inicial de Java
- Nivel de rastreo de Java
- Argumentos de JVM
- Vía de acceso de clases para archivos JAR externos
- El número de puerto de origen de datos de socket
- Valores de la vía de acceso de clases JMX o JDBC

Configuración avanzada de subnodos
Utilice la configuración avanzada de subnodo para alterar temporalmente una propiedad de configuración del agente en un subnodo.

Acerca de esta tarea

Existe una opción en IBM Tivoli Monitoring V6.2.1 y en los agentes posteriores que puede habilitar para alterar temporalmente las propiedades de cualquier sección de configuración de nivel de agente en una instancia de subnodo. En la página **Alteración temporal de configuración de subnodo** , hay un recuadro

de verificación etiquetado **Permitir que se altere temporalmente cualquier propiedad de configuración en cualquier subnodo**. Para obtener más información, consulte ("Alteraciones temporales de la configuración del subnodo" en la página 1393). Para que esta opción se habilite, debe seleccionar **6.2.1** como la **versión ITM mínima** cuando nombre al agente ("Denominación y configuración del agente" en la página 1205). Si se elige esta opción, cada instancia de subnodo puede alterar temporalmente cualquier propiedad de cualquier sección de configuración de nivel de agente. Sin embargo, esta propiedad se puede alterar temporalmente solo desde la GUI y no desde la línea de mandatos **`itmcmd`**.

Procedimiento

La opción **Permitir que se altere temporalmente cualquier propiedad de configuración en cualquier subnodo** hace que se visualice un campo **Avanzado** que contiene una lista en cada panel de configuración de subnodo. La selección inicial del campo **Avanzado** proporciona las instrucciones breves: **Seleccione una sección para alterar temporalmente valores**.

- Al pulsar en la lista, verá una lista de todas las secciones sin subnodo que contienen propiedades de configuración.
- Seleccione una sección

  Las propiedades de esta sección se añadirán temporalmente al panel de subnodo. El valor de cualquier propiedad que cambie se añade al conjunto de propiedades que se definen para el subnodo. El origen de datos de subnodo buscará valores de propiedad en el subnodo antes de buscar en las secciones de nivel de agente. .

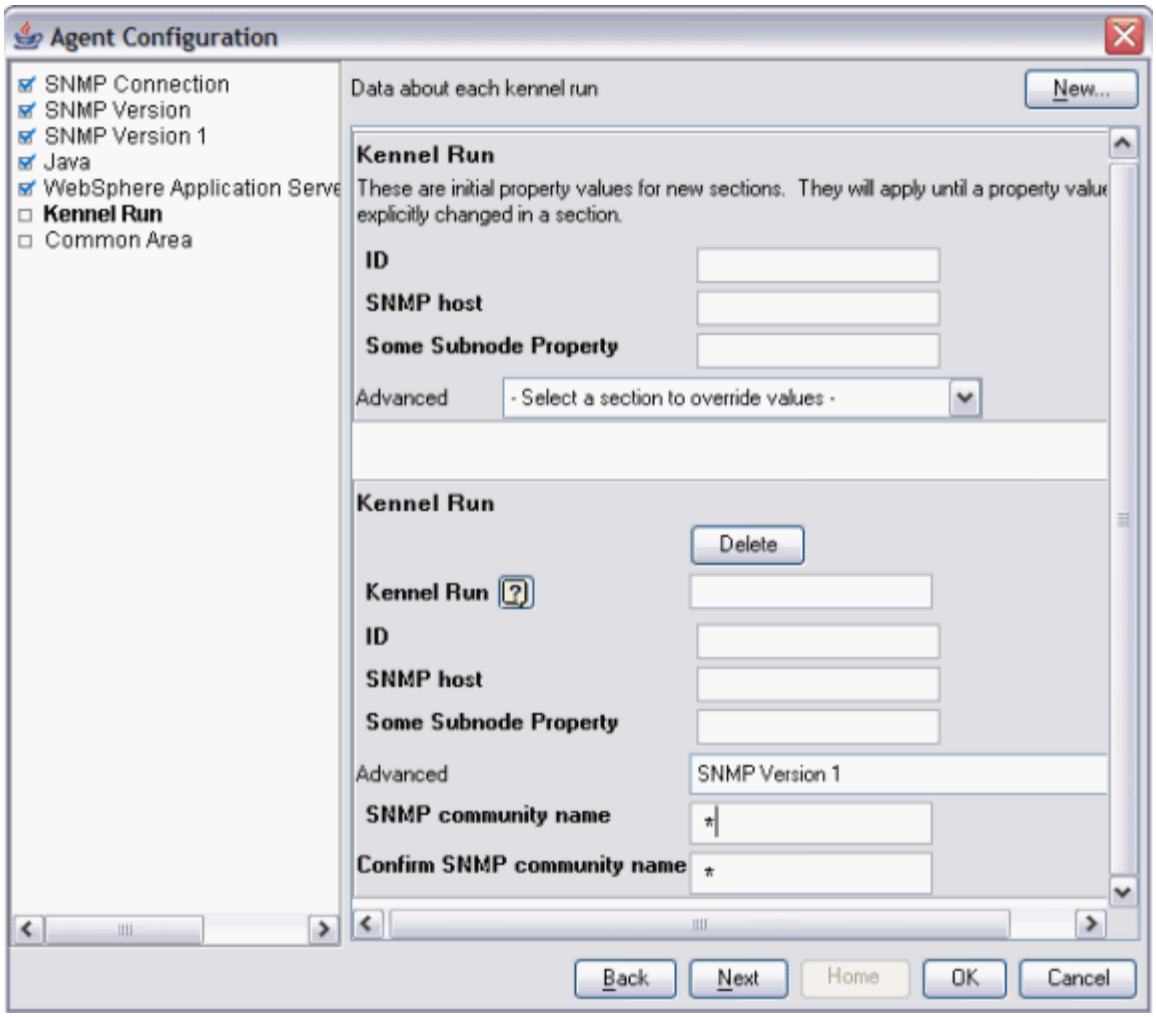


Figura 55. Propiedades ampliadas de SNMP Versión 1

La siguiente información adicional se aplica a las propiedades de alteración temporal de las secciones de nivel de agente:

- Las propiedades que se copian en la sección de subnodo no se muestran cuando se ha seleccionado la sección de nivel de agente en la lista **Avanzado**. Por ejemplo, en Figura 55 en la página 1394, el **host SNMP** no se visualiza después de la lista **Avanzado** porque se ha copiado en las propiedades de subnodo y ya se visualiza.
- Las secciones que no contienen propiedades que se puedan alterar temporalmente no tienen una selección en la lista **Avanzado**.
- Los valores sustituidos que se hayan entrado para una sección se guardarán si selecciona una sección diferente para mostrar propiedades diferentes.
- Seleccione **Permitir que se altere temporalmente cualquier propiedad de configuración en cualquier subnodo** para habilitar esta característica en el agente.

Configuración de un subnodo desde la línea de mandatos
En el entorno IBM Tivoli Monitoring, también puede configurar un subnodo utilizando la línea de mandatos.

Antes de empezar

Para obtener más información sobre la configuración de subnodos, consulte "Configuración del subnodo" en la página 1391

Acerca de esta tarea

Procedimiento

- Para configurar una instancia de subnodo desde la línea de mandatos, utilice el siguiente mandato:

```
tacmd configureSystem -m HOSTNAME:00 -p
nombre_sección:id_instancia_subnodo.nombre_propiedad=valor
```

  Donde:

  nombre_sección
  Igual que el tipo de subnodo

  id_instancia_subnodo
  ID del subnodo que se define durante la configuración.

  nombre_propiedad
  Nombre de la propiedad de configuración

  valor
  Valor de la propiedad

Ejemplo de configuración de subnodo
Cómo configurar un agente de muestra con un subnodo definido.

Ejemplo:

En este ejemplo se muestra cómo configurar un agente de muestra que tiene un subnodo llamado Subnodo de ejemplo de tipo `exs` y las tres propiedades de configuración siguientes:

- `Cfg agente` (el nombre de propiedad real es `K00_AGENT_CFG`) solo se define en el nivel de agente.
- `Cfg subnodo` (el nombre de propiedad real es `K00_SUBNODE_CFG`) solo se define en el subnodo de ejemplo.
- `Cfg alterable temporalmente` (el nombre de propiedad real es `K00_OVERRIDABLE_CFG`) se define en el nivel de agente y se ha copiado en el subnodo de ejemplo.

La Figura 56 en la página 1396 muestra estas propiedades de configuración en la página **Información de configuración de tiempo de ejecución** de Agent Editor.

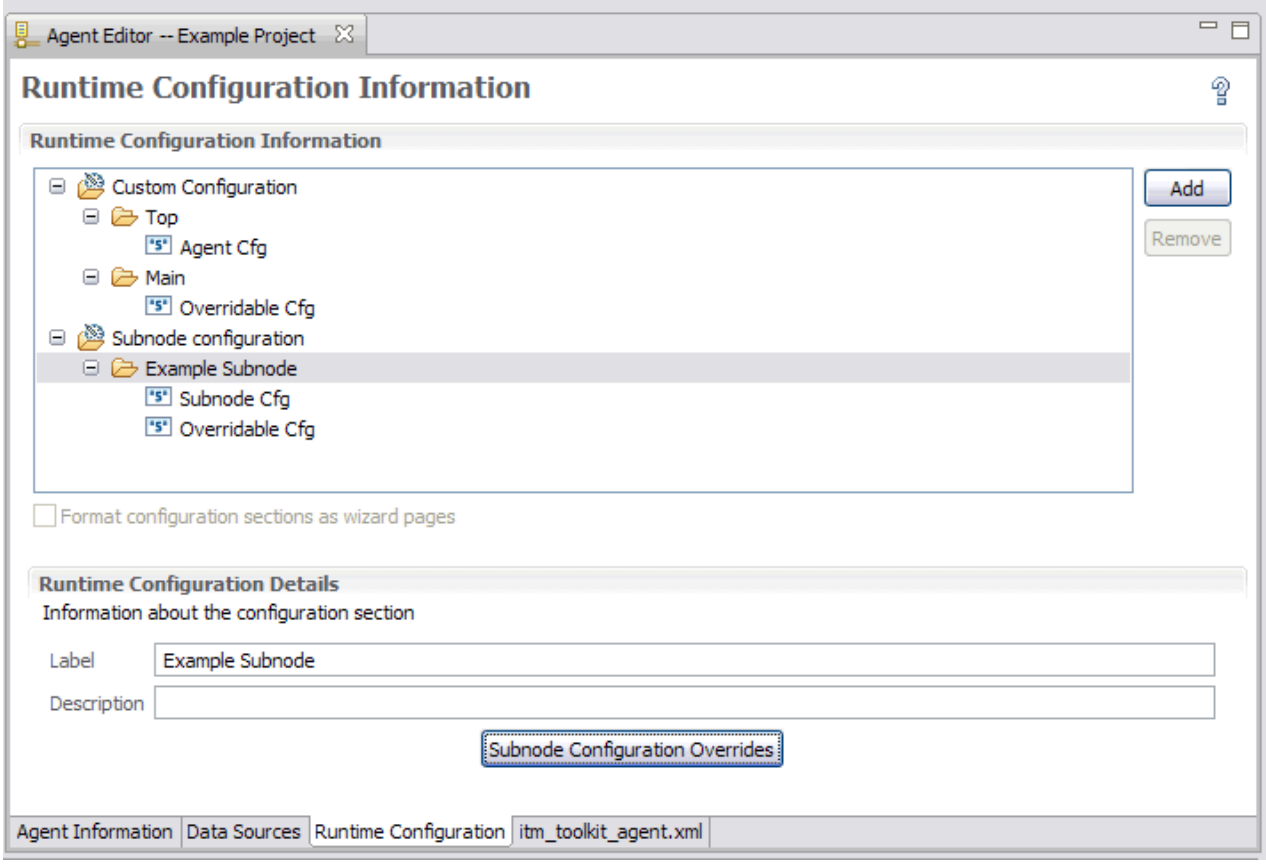


Figura 56. Definiciones de propiedades de configuración en Agent Builder

Cuando este agente de ejemplo se configura, la primer página que se muestra es la sección **superior** ,la cual contiene la propiedad **Cfg agente** como se muestra en (Figura 57 en la página 1397). Puesto que se trata de una propiedad de nivel de agente, se muestra una vez durante la configuración del agente. Cualquier instancia del Subnodo de ejemplo puede ver el valor de esta propiedad, pero todas las instancias ven el mismo valor.

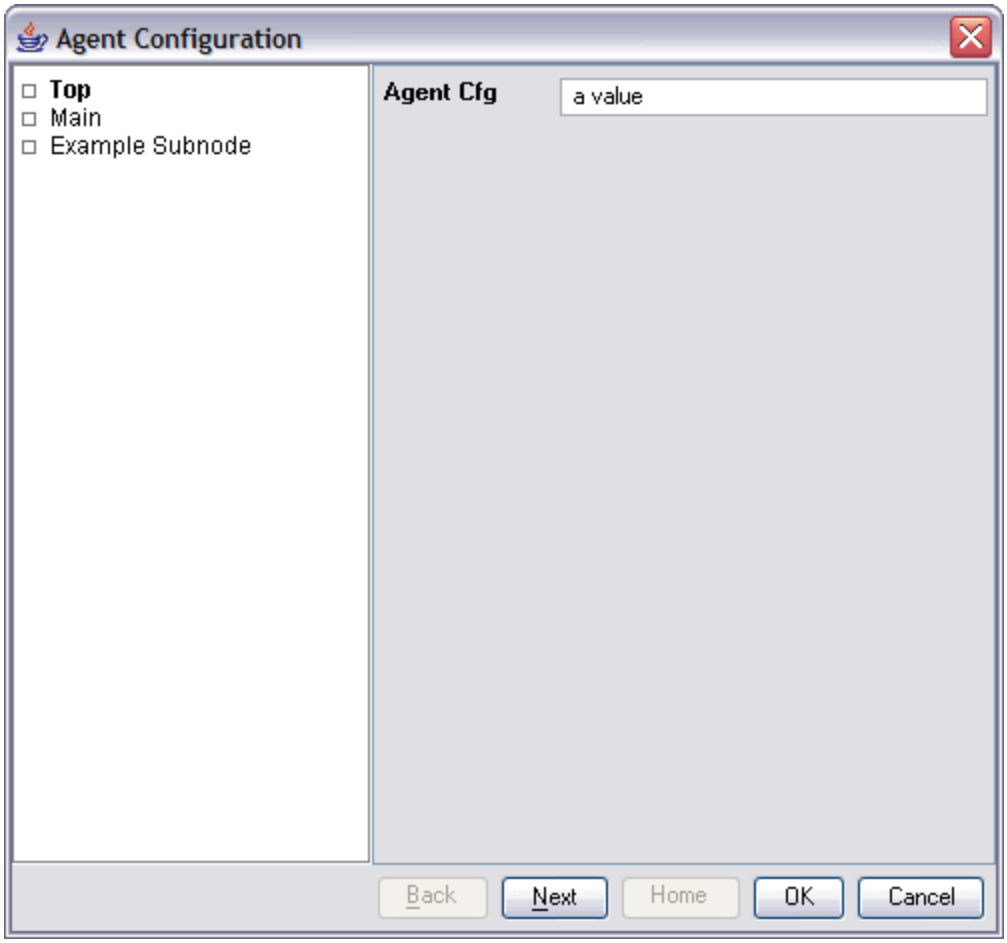


*Figura 57. Sección **Superior** con configuración a nivel de agente para la propiedad **Agent Cfg***

Si configura desde la línea de mandatos de Tivoli Enterprise Monitoring Server, se puede establecer la propiedad **Cfg agente** con el mandato siguiente:

```
tacmd configureSystem -m HOSTNAME:00 -p "TOP.K00_AGENT_CFG=a value"
```

La siguiente sección que se visualiza es la sección **Principal** tal como se muestra en la Figura 58 en la página 1398. También es una sección a nivel de agente y contiene la propiedad a nivel de agente **Overridable Cfg**. Esta propiedad difiere de la propiedad **Cfg agente** en que esta propiedad se ha copiado en el Subnodo de ejemplo en Agent Builder. Esto significa que se puede especificar un valor predeterminado de la propiedad en la página **Principal**. Sin embargo, cualquier instancia de Subnodo de ejemplo puede alterar temporalmente el valor que se especifica aquí por otro diferente.

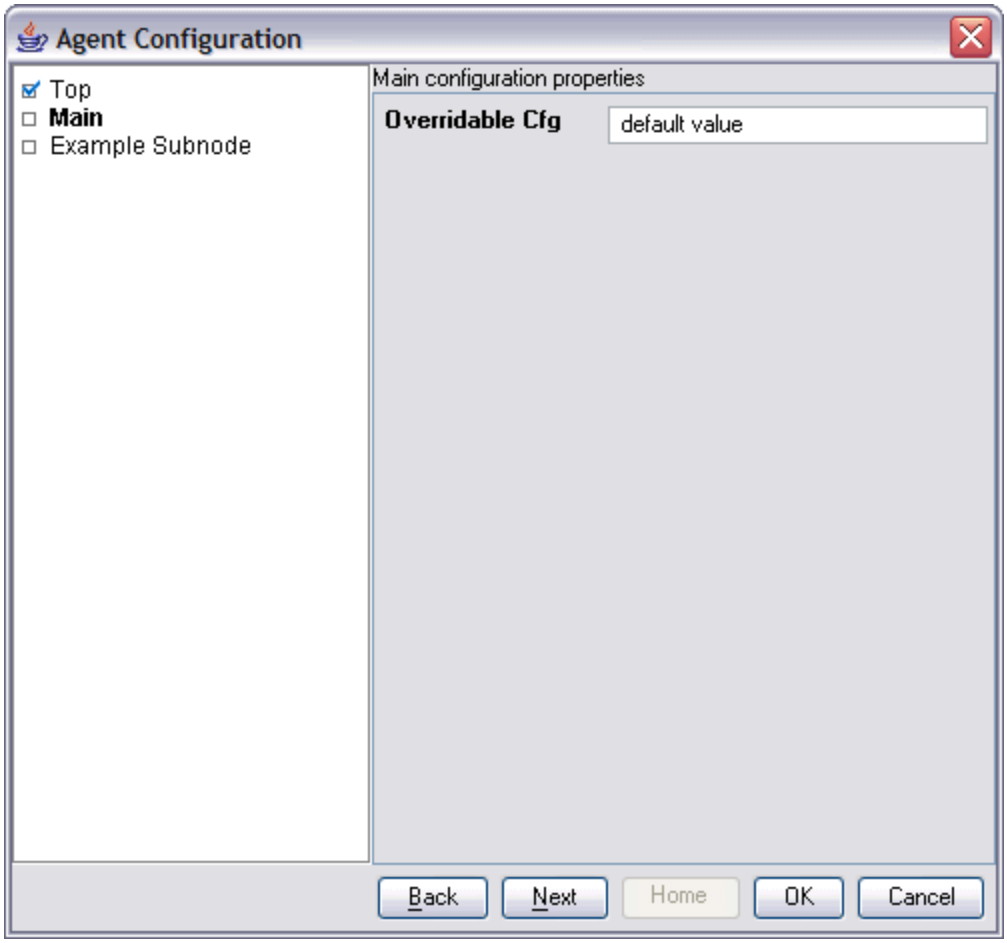


*Figura 58. Sección **Principal** con valor predeterminado de nivel de agente para la propiedad **Overridable Cfg***

Si realiza la configuración desde la línea de mandatos de Tivoli Enterprise Monitoring Server, esta propiedad se puede establecer utilizando el mandato siguiente:

```
tacmd configureSystem -m HOSTNAME:00 -p "MAIN.K00_OVERRIDABLE_CFG=default value"
```

Puede colocar ambas propiedades en la misma sección a nivel de agente. Puede decidir el número de secciones personalizadas a nivel de agente que desea crear y cómo distribuir entre las mismas las propiedades personalizadas.

La siguiente sección que se visualiza es la sección **Subnodo de ejemplo** tal como se muestra en la Figura 59 en la página 1399. Dado que este agente se configura por primera vez, no hay instancias de subnodo definidas y no se muestran subsecciones de instancia de subnodo. Se muestra la subsección de valores iniciales de propiedades, aunque es opcional y puede que algunos tipos de subnodo no se muestren. Puesto que se muestra la subsección de valores iniciales de propiedades, se pueden especificar valores predeterminados para cualquiera de las propiedades de configuración. La propiedad **Cfg alterable temporalmente** ya tiene un valor predeterminado que se ha obtenido de la propiedad de nivel de agente del mismo nombre.

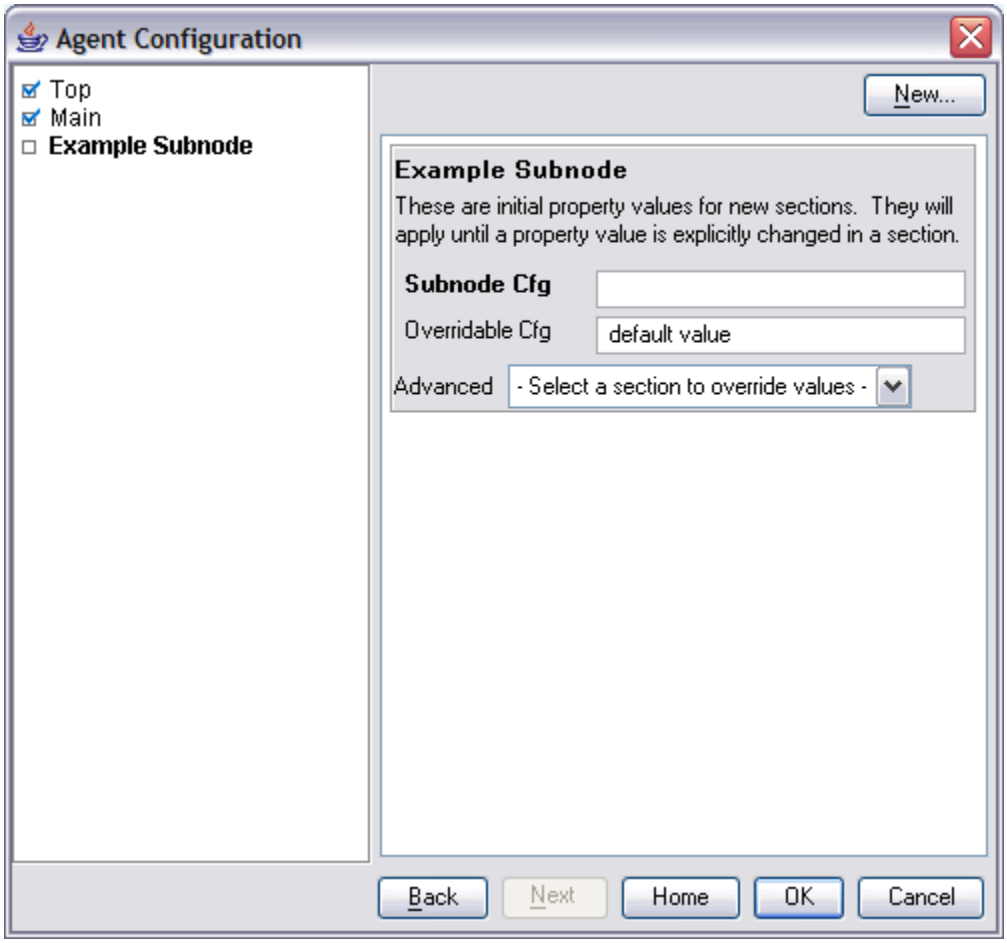


*Figura 59. Página de sección **Subnodo de ejemplo** sin subnodos*

Las instancias de subnodo se definen realizando las acciones siguientes en la página de sección vacía de **Subnodo de ejemplo** (Figura 60 en la página 1400):

1. En la sección **Subnodo de ejemplo** inicial, en el campo **Subnode Cfg**, escriba la siguiente serie predeterminada para la propiedad: `sub-default value`.
2. Pulse **Nuevo**. Una subsección de **Subnodo de ejemplo** se visualiza después de la subsección de propiedades iniciales.
3. En el campo **Subnodo de ejemplo**, escriba el siguiente ID de instancia de subnodo: do.
4. Pulse **Nuevo**. Una segunda subsección de **Subnodo de ejemplo** se muestra después de la primera.
5. En el segundo campo **Subnodo de ejemplo**, escriba el siguiente ID de instancia de subnodo: `re`.
6. En el campo **Cfg subnodo**, escriba el siguiente valor para la propiedad **Cfg subnodo**: `sc override`.
7. En el campo **Cfg alterable temporalmente**, escriba el siguiente valor para la propiedad **Cfg alterable temporalmente**: `oc override`.

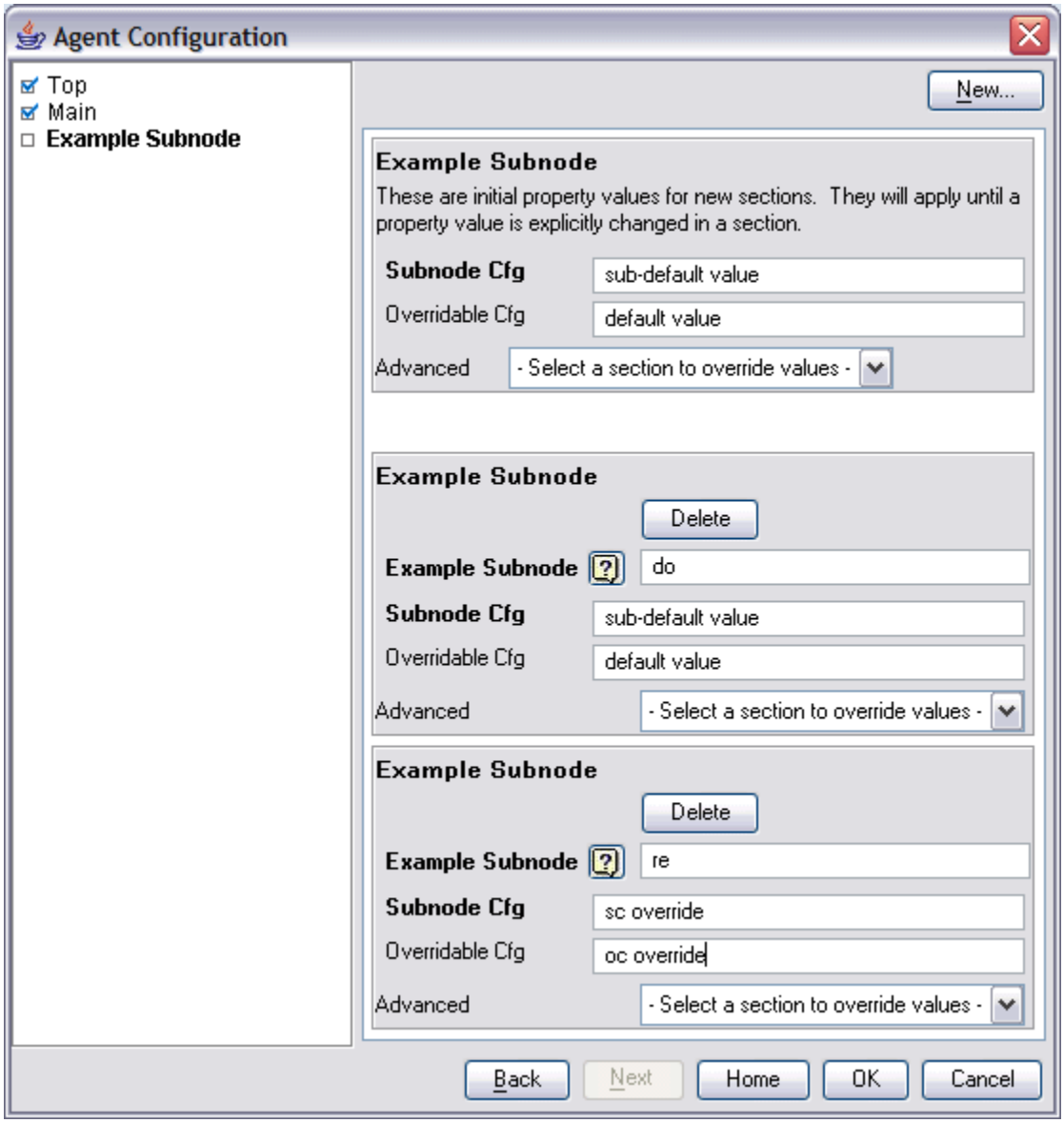


*Figura 60. Página de sección **Subnodo de ejemplo** con dos instancias de subnodo definidas*

Las dos nuevas subsecciones hacen que el agente cree dos instancias de subnodo cuando se inicia. Puesto que las propiedades de la subsección de subnodo **do** no se han modificado, dicha instancia de subnodo utiliza los valores de propiedad predeterminados. Como se han especificado distintos valores para las propiedades de la subsección **re**, la instancia de subnodo **re** utiliza dichos valores especificados.

Puede definir un valor predeterminado desde la línea de mandatos del Tivoli Enterprise Monitoring Server con el siguiente mandato:

```
tacmd configureSystem -m HOSTNAME:00 -p "exs.K00_SUBNODE_CFG=sub-default value"
```

El formato para definir valores predeterminados de subnodo es exactamente igual que el formato para definir propiedades a nivel de agente, excepto en que el nombre de sección identifica una sección de subnodo.

Puede crear las instancias de subnodo desde la línea de mandatos del Tivoli Enterprise Monitoring Server con el siguiente mandato:

```
tacmd configureSystem -m HOSTNAME:00 -p "exs:do.K00_OVERRIDABLE_CFG=default value" \
 "exs:re.K00_SUBNODE_CFG=sc override" "exs:re.K00_OVERRIDABLE_CFG=oc override"
```

El ID de la instancia de subnodo se inserta entre el nombre de sección y el nombre de propiedad. Cuando utiliza la línea de mandatos para crear una instancia de subnodo al menos una propiedad debe especificarse, incluso si todas las propiedades utilizan valores predeterminados. De lo contrario, no es necesario especificar los valores predeterminados en la línea de mandatos cuando se definen las instancias de subnodo.

Todas las propiedades de configuración del agente se pueden definir en un solo mandato. El siguiente mandato es equivalente a todos los mandatos individuales anteriores:

```
tacmd configureSystem -m HOSTNAME:00 -p "TOP.K00_AGENT_CFG=a value" \
 "MAIN.K00_OVERRIDABLE_CFG=default value" \
 "exs.K00_SUBNODE_CFG=sub-default value" \
 "exs:do.K00_OVERRIDABLE_CFG=default value" \
 "exs:re.K00_SUBNODE_CFG=sc override" "exs:re.K00_OVERRIDABLE_CFG=oc override"
```

Subnodos y orígenes de datos de Windows
Elija si desea incluir propiedades de conexión remota a Windows en el agente o no.

Acerca de esta tarea

Si un agente tiene orígenes de datos de Windows en el nivel de agente y no en los subnodos, la inclusión de propiedades de configuración de conexión remota a Windows es opcional. Los orígenes de datos de Windows son el registro de sucesos de Windows, Windows Management Instrumentation y el supervisor de rendimiento de Windows. Si las propiedades de configuración no se incluyen, estos orígenes de datos supervisan el sistema Windows local de forma predeterminada y no es necesaria ninguna configuración. De forma predeterminada, no se incluye ningún origen de datos de Windows en ningún subnodo.

Para decidir si deben incluirse propiedades de Conexión al sistema Windows remoto en el agente, siga estos pasos:

Procedimiento

1. En la página **Información de Windows Management Instrumentation (WMI)** , pulse **Opciones globales** cuando se muestren las propiedades de origen de datos. Seleccione **Opciones globales** mientras crea el origen de datos o desde la página **Orígenes de datos** de Agent Editor.
2. En la ventana **Opciones globales de origen de datos de Windows**, seleccione **Incluir configuración de conexión remota de Windows** si desea incluir estas propiedades en el agente.

Subnodos y orígenes de datos de script
Los scripts de subnodo acceden a las propiedades de configuración de instancia de subnodo del mismo modo que en los scripts de nivel de agente.

Lo scripts tienen acceso a todas las propiedades de configuración de nivel de agente y a todas las propiedades de configuración de instancia de subnodo. Si se altera temporalmente una propiedad de nivel de agente en el nivel de subnodo, el script únicamente tiene acceso al valor de propiedad de nivel de subnodo.

Personalización de la configuración del agente

Personalice la configuración del proceso, el archivo de registro y los orígenes de datos de script.

Antes de empezar

Si está añadiendo orígenes de datos SNMP, JMX, CIM, JDBC, HTTP y SOAP al agente, configure estos orígenes de datos tal como se describe en las secciones siguientes:

- “Supervisión de datos procedentes de un servidor de protocolo simple de gestión de red (SNMP)” en la página 1267
- “Supervisión de MBeans Java Management Extensions (JMX)” en la página 1278
- “Supervisión de datos procedentes de un CIM (Common Information Model)” en la página 1297

- "Supervisión de datos procedentes de JDBC (Java Database Connectivity)" en la página 1325
- "Supervisión de la disponibilidad de HTTP y del tiempo de respuesta" en la página 1335
- "Supervisión de datos de un origen de datos SOAP u otro origen de datos HTTP" en la página 1344

Acerca de esta tarea

Utilice esta tarea para personalizar la configuración de los orígenes de datos de proceso, archivo de registro y script para que un agente pueda acceder a la aplicación que está supervisando.

Todos los agentes deben estar configurados para que se puedan iniciar. Todos los agentes deben tener información de configuración básica como, por ejemplo, el método de conexión con el Tivoli Enterprise Monitoring Server. Muchas veces, un agente debe tener más información de configuración para poder acceder a información específica del sistema en el que se ejecuta. Por ejemplo, si necesita conocer la ubicación de instalación de un producto de software, añada propiedades de configuración para solicitar esta información. Otro ejemplo de información que puede solicitar es el ID de usuario y contraseña para acceder a una interfaz.

La configuración personalizada la define el desarrollador de agentes. Si es necesaria para todos los agentes, pero se puede utilizar en las siguientes áreas de recopilación de datos:

- Coincidencia con un argumento de un Supervisor de proceso
- Coincidencia con la línea de mandatos de un Supervisor de proceso
- Formación de una vía de acceso o nombre de archivo de registro
- Definición de una variable de entorno en un script

Nota: Determinados orígenes de datos, como por ejemplo JMX y SNMP, añaden esta configuración automáticamente.

Nota: Cuando Agent Builder añade automáticamente la configuración específica de origen de datos, dicha configuración sólo se añade en inglés.

Si durante la definición del origen de datos el agente necesita información específica del sistema para un área de recopilación de datos, se muestra **Insertar propiedad** o **Insertar propiedad de configuración**.

Por ejemplo, cuando crea un grupo de atributos que supervisa un archivo de registro, se muestra **Insertar propiedad de configuración**.

Procedimiento

1. Pulse **Insertar propiedad de configuración** para mostrar la ventana **Propiedades de configuración**,
2. En la ventana **Propiedades de configuración**, pulse una propiedad y pulse **Añadir**.

   Nota: Inicialmente no hay propiedades de configuración definidas para el agente.
3. En la ventana **Propiedad de configuración de tiempo de ejecución**, complete los campos siguientes:
   a) En el área **Sección**, complete los campos siguientes:

      Etiqueta
      Texto que describe las propiedades

      Descripción
      (opcional) Descripción de las propiedades

   b) En el área **Propiedad**, complete los campos siguientes:

      Etiqueta
      Texto que se visualiza en el panel de configuración del agente que identifica la información que debe entrar.

      Variable de entorno
      La variable de entorno se muestra en el campo **Variable de entorno** y se actualiza a medida que se escribe en el campo de etiqueta. Agent Builder construye automáticamente el nombre de la variable de entorno a partir del código del producto y de la etiqueta. Si desea cambiar la variable de entorno independientemente de la etiqueta, puede borrar **Coincidir con etiqueta**.

Descripción
(opcional) Descripción de la propiedad que se define.

Tipo
Tipo de información recopilada, una de las opciones siguientes:

Serie
Para cualquier información alfabética que se deba recopilar (por ejemplo, ubicaciones de instalación, nombres de usuario y nombres de host).

Contraseña
Para cualquier información que deba cifrarse cuando se almacene. Además de proporcionar el cifrado de los datos, los datos introducidos en el recuadro de texto se oscurecen mediante asteriscos. Además, el usuario debe escribir esta información dos veces para validar los datos.

Numérico
Para cualquier información numérica (por ejemplo, números de puerto).

Opción
Para una lista de valores especificados. Esta opción habilita la tabla Opciones. Puede definir valores específicos pulsando **Añadir**. Los valores especificados se visualizan en el panel de configuración del agente como un grupo de selecciones, solo se puede realizar una selección en el grupo.

Texto de sólo lectura
Muestra el texto al configurar el agente, pero no se recopila información.

Separador
Muestra un separador horizontal, pero no se recopila información.

Navegador de archivos
Recopila una serie que es un nombre de archivo. Pulse **Examinar** para examinar el sistema de archivos para el archivo que se desea.

Valor predeterminado
(Opcional) Especifique el valor que se muestra en el panel de configuración en tiempo de ejecución cuando se configura por primera vez al agente. Si se desea un valor predeterminado para UNIX/Linux que sea distinto que un valor predeterminado para Windows, pulse **Varios valores**.

En la ventana **Valores predeterminados de propiedad de configuración**, especifique los valores predeterminados que desea para los sistemas Windows y para los sistemas UNIX y Linux.

Nota: El soporte para varios valores predeterminados es una función a la que sólo se da soporte en IBM Tivoli Monitoring V6.2.1 y posterior. Si el agente es compatible con IBM Tivoli Monitoring V6.2, una solicitud le avisa de este requisito y puede cancelar o continuar con la compatibilidad de V6.2.1 habilitada.

Necesario
Seleccione este campo si el usuario debe especificar un valor al configurarse el agente. Borre este campo si el especificar un valor es opcional para el usuario.

c) Para añadir una opción, pulse en **Añadir**

4. En la ventana **Valor de propiedad de configuración**, complete los campos **Etiqueta** y **Valor**.

   La Etiqueta se visualiza como una de las opciones. Si toma esta opción, el valor se convierte en la valor de la propiedad.

5. Pulse **Aceptar**.

   La nueva sección de configuración y propiedad se visualizan en la ventana **Propiedades de configuración** en **Configuración personalizada**.

6. Opcional: Para añadir otra propiedad a una sección existente, seleccione la sección o una propiedad existente en la sección y pulse **Añadir**. La selección se realiza en el árbol de configuración de tiempo de ejecución de la ventana **Propiedades de configuración**.

7. Rellene los campos correspondientes a la nueva propiedad. (Complete los mismos campos como en el paso "3" en la página 1402).
8. Pulse **Aceptar**. Se selecciona la propiedad que añadió más recientemente.
9. Guarde la selección o seleccione la propiedad que desea insertar en el nombre de archivo de registro.
10. Pulse **Aceptar**. La propiedad se inserta en el nombre de archivo de registro.

    Puede continuar utilizando el asistente para completar la definición del grupo de atributos de archivo de registro.

    Nota: Aunque se defina una propiedad de configuración en el contexto de un nombre de archivo de registro, se puede utilizar en otras ubicaciones. Por ejemplo, otra ubicación que acepta una propiedad de configuración es un origen de datos de script. Esta flexibilidad significa que puede acceder al valor para el elemento de configuración **Información de archivo** con la variable de script *$K00_APPLICATION_LOG_FILE* si el código de producto es K00. También puede utilizar la variable de archivo por lotes de Windows *%K00_APPLICATION_LOG_FILE%*.

Cambio de las propiedades de configuración utilizando Agent Editor

Utilice Agent Editor para cambiar las propiedades de configuración del agente.

Acerca de esta tarea

Esta tarea proporciona información sobre la visualización, la adición y el cambio de las propiedades de configuración utilizando Agent Editor.

Procedimiento

1. Pulse el separador **Configuración de tiempo de ejecución**.
2. Seleccione una sección de configuración y pulse en **Añadir**.

   Añadir funciona igual que lo hace en "Personalización de la configuración del agente" en la página 1401. No hay ninguna selección de **Editar** porque una sección de configuración o propiedad se edita cuando se selecciona.
3. Seleccione una propiedad de configuración para visualizar el área **Detalles de configuración de tiempo de ejecución**.
4. En el área **Detalles de configuración de tiempo de ejecución**, edite los campos para configurar la propiedad.

Configuración de una conexión remota de Windows

Información sobre la configuración de una conexión remota de Windows

Acerca de esta tarea

Los orígenes de datos de Windows Management Instrumentation (WMI), el Supervisor de rendimiento de Windows Performance Monitor (Perfmon) y el registro de sucesos de Windows pueden supervisar los datos del sistema donde el agente está instalado. Estos orígenes de datos también pueden supervisar datos en sistemas Windows remotos. Estos tres tipos de orígenes de datos se denominan orígenes de datos de Windows. Si estos orígenes de datos de Windows supervisan datos remotamente, todos ellos comparten las propiedades de configuración de conexión remota de Windows para el nivel de agente donde están definidos.

Si define un origen de datos de Windows en el nivel base del agente, las propiedades de configuración de la conexión remota de Windows no se añaden al agente automáticamente. No se añaden para mantener la compatibilidad con versiones anteriores de agentes que puedan utilizar el proveedor de datos de Windows antes de habilitar la supervisión remota. El origen de datos de Windows del agente supervisa datos en el sistema Windows local en el que está instalado el agente.

Si define un origen de datos de Windows en un subnodo del agente, las propiedades de configuración de la conexión remota de Windows se añaden al agente automáticamente. El origen de datos de Windows debe soportar la conexión remota de Windows si es un subnodo. No puede borrar la opción hasta que

todos los orígenes de datos de Windows se eliminan de todos los subnodos del agente. Cada instancia de un subnodo puede configurarse para supervisar un sistema Windows remoto diferente. Todos los orígenes de datos de Windows del subnodo comparten las propiedades de configuración de conexión remota de Windows.

Para configurar un agente base para que supervise remotamente un único sistema remoto Windows, utilice el siguiente procedimiento.

Procedimiento

1. En la ventana **Definición de origen de datos** de Agent Editor, pulse **Opciones globales**.
   Se abre la ventana **Opciones globales de origen de datos de Windows**.
2. Seleccione **Incluir configuración de conexión remota de Windows**.
3. Pulse **Aceptar**.

Resultados

Las siguientes propiedades de configuración específicas de la conexión se pueden acceder desde la página **Información de configuración de tiempo de ejecución** de Agent Editor, seleccionando **Configuración del acceso remoto de Windows** > **Conexión remota de Windows**

Host remoto de Windows
Nombre de host del sistema remoto Windows

Contraseña remota de Windows
Contraseña para Windows remoto

Windows `DOMINIO\nombre usuario` remoto
Nombre de usuario del host Windows remoto

Qué hacer a continuación

Puede ver, añadir y cambiar las propiedades de configuración utilizando Agent Editor. Encontrará instrucciones en: "Cambio de las propiedades de configuración utilizando Agent Editor" en la página 1404. Si un origen de datos de Windows se ha definido en un subnodo, también puede especificar Alteraciones temporales de configuración de subnodo. Encontrará instrucciones en: "Configuración del subnodo" en la página 1391.

Creación de un usuario con permisos de Windows Management Instrumentation (WMI)

Puede añadir y configurar un usuario en un sistema Windows con permisos para permitir la exploración WMI.

Acerca de esta tarea

Si el agente recopila datos de un sistema remoto utilizando Windows Management Instrumentation (WMI), necesita permisos para acceder a datos WMI en el sistema remoto. El agente puede acceder a datos WMI de un sistema remoto cuando se proporcionan credenciales de una cuenta con permisos para acceder a datos WMI del sistema. El procedimiento se aplica a Windows 7, Windows 2008 Server y Windows Vista.

Nota: El agente también puede acceder a datos en un sistema remoto Windows al utilizar los orígenes de datos del Supervisor de rendimiento de Windows (Perfmon) y del Registro de sucesos de Windows. Sin embargo, en el caso de los orígenes de datos del Supervisor de rendimiento de Windows (Perfmon) y en el Registro de sucesos de Windows, debe proporcionar las credenciales de Administrador para el sistema remoto.

Procedimiento

1. Cree una cuenta de usuario:

a. Vaya a Windows **Inicio** > **Herramientas administrativas** > **Gestión de sistemas**. Se abre la ventana **Gestión de sistemas**.
b. Expanda **Usuarios locales y grupos**.
c. Pulse el botón derecho (del ratón) en la carpeta **Usuarios** y seleccione **Nuevo usuario**.
d. Complete los detalles del usuario y pulse **Crear** y **Cerrar**.

2. Configure la pertenencia a grupos para la cuenta de usuario nuevo:
   a. En la ventana **Gestión de sistemas**, seleccione la carpeta **Usuarios**.
   b. Pulse con el botón derecho del ratón la cuenta de usuario nuevo y seleccione **Propiedades**.
   c. Pulse la pestaña **Miembro de**.
   d. Pulse **Añadir**.
   e. Pulse **Opciones avanzadas**.
   f. Pulse **Buscar ahora**.
   g. Seleccione los siguientes grupos:
      - Usuarios de COM distribuidos
      - Usuarios de registro de rendimiento
      - Usuarios de escritorio remoto

      Consejo: Pulse Control y pulse para seleccionar varios grupos.
   h. Pulse **Aceptar** hasta volver a la ventana **Gestión de sistemas**.
   i. Seleccione **Archivo** > **Salir** para salir de la ventana **Gestión de sistemas**.
3. Asigne derechos de Modelo de objetos componentes distribuido (DCOM):
   a. Vaya a Windows **Inicio** > **Herramientas administrativas** > **Servicios de componentes**. Se abre la ventana **Servicios de componentes**.
   b. Expanda **Servicios de componentes** > **Sistemas** > **Mi PC**.
   c. Pulse con el botón derecho del ratón sobre **Mi PC** y seleccione **Propiedades**. Se abre la ventana **Propiedades de Mi PC**.
   d. Pulse la pestaña **Seguridad COM**.
   e. En el área **Permisos de acceso**, pulse **Editar límites**
   f. En **Usuarios COM distribuidos**, verifique que **Acceso local** y **Acceso remoto** estén seleccionados.
   g. Pulse **Aceptar** para guardar la configuración.
   h. En la ventana **Propiedades de Mi PC**, área de **Permisos de inicio y activación**, pulse **Editar límites**
   i. En **Usuarios COM distribuidos**, verifique que **Inicio local**, **Inicio remoto**, **Activación local** y **Activación remota** estén seleccionadas.
   j. Pulse **Aceptar** para guardar los valores y vuelva a pulsar **Aceptar** para cerrar la ventana **Propiedades de Mi PC**.
   k. Seleccione **Archivo** > **Salir** para salir de la ventana **Servicios de componentes**.
4. Configure las asignaciones de seguridad del espacio de nombres WMI
   a. Vaya a Windows **Inicio** > **Ejecutar...**.
   b. Especifique `wmimgmt.msc` y pulse **Aceptar**.
   c. Pulse con el botón derecho del ratón sobre **Control WMI (Local)** y seleccione **Propiedades**.
   d. Pulse la pestaña **Seguridad**.
   e. Pulse **Seguridad**.
   f. Pulse **Añadir**.
   g. Pulse **Opciones avanzadas**.

h. Pulse **Buscar ahora**.
i. Seleccione la cuenta de usuario nuevo y pulse **Aceptar** hasta volver a la ventana **Seguridad para raíz**.
j. Pulse **Opciones avanzadas** y seleccione la cuenta de usuario que acaba de añadir.
k. Pulse **Editar**.
l. En la selección de menús **Aplicar a:**, seleccione **Este espacio de nombres y subespacios de nombres**.
m. En **Ejecutar métodos**, verifique que **Habilitar cuenta**, **Habilitación remota** y **Seguridad de lectura** estén seleccionadas.
n. Pulse **Aceptar** hasta que vuelva a la ventana de **wmimgmt**.
o. Seleccione **Archivo** > **Salir** para salir de la ventana de **wmimgmt**.

Qué hacer a continuación

Para obtener más información sobre la recopilación de datos de WMI desde un sistema remoto, consulte "Supervisión de datos de Windows Management Instrumentation (WMI)" en la página 1263.

Configuración de una conexión remota de Secure Shell (SSH)

Información sobre la configuración de una conexión remota de SSH

Acerca de esta tarea

Los orígenes de datos de script pueden supervisar datos en el sistema en el que esté instalado el agente y también en sistemas remotos. Si los orígenes de datos de script supervisan datos remotamente, todos comparten propiedades de configuración de conexión remota SSH para el nivel de agente en el que están definidos. Las versiones anteriores de un agente pueden utilizar el proveedor de daros de script antes de habilitar la supervisión remota. Para mantener la compatibilidad con versiones anteriores de agentes, las propiedades de configuración de conexión remota SSH no se añaden automáticamente al agente. El origen de datos de script del agente supervisa los datos del sistema local en el que esté instalado el agente.

Si define un origen de datos de script en un subnodo y selecciona **Habilitar recopilación de datos utilizado SSH**, puede configurar cada instancia de subnodo para que supervise un sistema remoto diferente. Todos los orígenes de datos de script del subnodo comparten las propiedades de configuración de conexión remota de SSH.

Si desea que el agente supervise remotamente un sistema remoto, utilice el procedimiento siguiente.

Procedimiento

En la ventana **Definición de orígenes de datos** del Agent Editor para el origen de datos de script, seleccione **Habilitar recopilación de datos utilizando SSH**.

Resultados

Las siguientes propiedades de configuración específicas de la conexión se pueden acceder desde **Agent Editor**, página **Información de configuración de tiempo de ejecución**, seleccionando **Configuración para Secure Shell (SSH)** > **Conexión remota de SSH**

Dirección de red
La dirección IP o el nombre de host del sistema remoto.

Número de puerto de SSH
El número de puerto IP en el que se ejecuta el servidor SSH. El valor predeterminado es 22.

Tipo de autenticación
Tipo de autenticación que se utiliza al iniciar sesión en el servidor SSH remoto. Puede elegir Contraseña o Clave pública.

Desconectarse del sistema remoto después de cada intervalo de recopilación
Una opción para determinar si el proveedor de datos de script descarta la sesión de inicio de sesión en el sistema remoto después de recopilar datos. De forma predeterminada, el valor es No.

Eliminar el script del sistema remoto después de cada intervalo de recopilación
Una opción para suprimir el script del sistema remoto después de cada intervalo de recopilación de datos. De forma predeterminada, el valor es No.

Si el tipo de autenticación se establece en Contraseña, se puede acceder a las siguientes propiedades de configuración desde **Agent Editor**, página **Información de configuración de tiempo de ejecución** seleccionando **Configuración para Secure Shell (SSH)** > **Contraseña**:

Nombre de usuario
Nombre de usuario para el sistema remoto

Contraseña
Contraseña para el sistema remoto

Si el tipo de autenticación se establece en clave pública, se puede acceder a las siguientes propiedades de configuración desde **Agent Editor**, página **Información de configuración de tiempo de ejecución** seleccionando **Configuración para Secure Shell (SSH)** > **Clave pública**:

Nombre de usuario
Nombre de usuario asociado con el archivo de clave pública

Archivo de claves públicas
Archivo de claves públicas asociado con el usuario

Archivo de claves privadas
Archivo de claves privadas asociado con el usuario

Contraseña
Contraseña utilizada para desbloquear el archivo de claves privadas

Qué hacer a continuación

Puede ver, añadir y cambiar las propiedades de configuración utilizando Agent Editor. Encontrará instrucciones en: "Cambio de las propiedades de configuración utilizando Agent Editor" en la página 1404. Si las propiedades de configuración de conexión remota de SSH se incluyen en un subnodo, también podrá especificar alteraciones temporales de configuración de subnodo. Encontrará instrucciones en: "Configuración del subnodo" en la página 1391.

Creación de espacios de trabajo, mandatos de Actuación y situaciones

Tras instalar un agente en un entorno IBM Tivoli Monitoring, puede crear espacios de trabajo, consultas, mandatos de actuación y situaciones para su solución de supervisión.

Las situaciones, espacios de trabajo, mandatos de Actuación y consultas que se crean se pueden incluir en el paquete de instalación. Para tener una imagen de instalación para las situaciones, los espacios de trabajo y el propio agente, los archivos de las situaciones y espacios de trabajo deben encontrarse en el mismo proyecto que el agente. Agent Builder incluye un asistente para crear los archivos apropiados en el proyecto del agente. Para obtener información sobre la importación de los archivos de soporte de aplicaciones, consulte "Importación de archivos de soporte de aplicaciones" en la página 1444.

Creación de situaciones, mandatos de Actuación y consultas

Encuentre información de ayuda para crear situaciones, mandatos de actuación y consultas.

Para crear situaciones, mandatos de actuación y consultas, utilice Tivoli Enterprise Portal y el editor de situaciones incluido. Para obtener información detallada sobre cómo crear situaciones y consultas, consulte la Guía del usuario de Tivoli Enterprise Portal. También puede utilizar la documentación de ayuda que se instala con Tivoli Enterprise Portal Server. Un agente de supervisión de Agent Builder puede reconocer y realizar un proceso especial para un conjunto de mandatos de Actuación. Si desea más

información sobre estos mandatos de actuación especiales, consulte “Consulta de mandatos de Actuación” en la página 1546.

Las situaciones para los agentes del supervisor del sistema se crean de forma diferente de las situaciones de empresa con el editor de situaciones de Tivoli Enterprise Portal o el mandato **tacmd createSit**. Para los agentes supervisores del sistema, las situaciones privadas se crean en un archivo XML de configuración de situaciones privadas locales para el agente. Para obtener más información sobre la creación de situaciones para los agentes de supervisión del sistema, consulte "Situaciones privadas" en el capítulo "Autonomía del agente" de la publicación *IBM Tivoli Monitoring: Guía del administrador*.

Creación de espacios de trabajo

Coloque Tivoli Enterprise Portal en la modalidad de Administrador para crear espacios de trabajo que puede exportar e incluir en la solución.

Acerca de esta tarea

Cree los espacios de trabajo en el entorno en el que se utilizan. Cuando construye espacios de trabajo, cambie los valores de visualización en el sistema para crear espacios de trabajo con la resolución mínima que se utiliza normalmente en el entorno. Si se crean los espacios de trabajo con una resolución mayor, se pueden crear vistas que estén demasiado confusas para utilizarse razonablemente con resoluciones inferiores.

Para crear espacios de trabajo que se puedan exportar e incluir en la solución, Tivoli Enterprise Portal debe ponerse en modalidad de "Administrador". Para colocar Tivoli Enterprise Portal en modalidad de "Administrador" siga estos pasos:

Procedimiento

1. Vaya al directorio *ITM_INSTALL*/CNP y abra el archivo `cnp.bat`.

   Si ha utilizado la instalación predeterminada, el directorio es `C:\IBM\ITM\CNP`. En el archivo `cnp.bat`, debe actualizar la línea `set _CMD= %_JAVA_CMD%` de modo que incluya la opción `-Dcnp.candle.mode="$_KCJ_$"`.

   Si desea crear extensiones en sistemas Linux o AIX, utilice la siguiente vía de acceso:

   ```
   /opt/IBM/ITM/li263/cj/bin/cnp.sh
   ```

   Donde *li263* es el sistema operativo en el que se está ejecutando Tivoli Enterprise Portal.

   La línea `set _CMD= %_JAVA_CMD%` actualizada es parecida a la del siguiente ejemplo:

   ```
   set _CMD= %_JAVA_CMD% -Dcnp.candle.mode="$_KCJ_$" -Xms64m -Xmx256m -showversion -noverify
    -classpath %CPATH% -Dkjr.trace.mode=LOCAL -Dkjr.trace.file=C:\IBM\ITM\CNP\LOGS\kcjras1.log
   -Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dibm.stream.nio=true
   -Dice.net.maxPersistentConnections=16 -Dice.net.persistentConnectionTimeout=1
   -Dcnp.http.url.host=SKINANE -Dvbroker.agent.enableLocator=false  -Dnv_inst_flag=%NV_INST_FLAG
   %
   -Dnvwc.cwd=%NVWC_WORKING_DIR% -Dnvwc.java=%NVWC_JAVA% candle.fw.pres.CMWApplet
   ```

   Nota: El mandato se muestra aquí en varias líneas solo por razones de formato.
2. Abra un nuevo cliente de Tivoli Enterprise Portal e inicie sesión con el ID de usuario `sysadmin`.
3. Establezca el ID de usuario "sysadmin" en la modalidad "Administrador". En Tivoli Enterprise Portal, seleccione **Editar** > **Administrar usuarios**. Seleccione **sysadmin** y, en el separador **Permisos**, seleccione **Administración de espacios de trabajo**. Marque el recuadro de selección **Modalidad de administración de espacios de trabajo**.

   Si realiza la selección correctamente, se visualiza ***MODALIDAD DE ADMINISTRACIÓN*** se visualiza en la barra de título del escritorio.

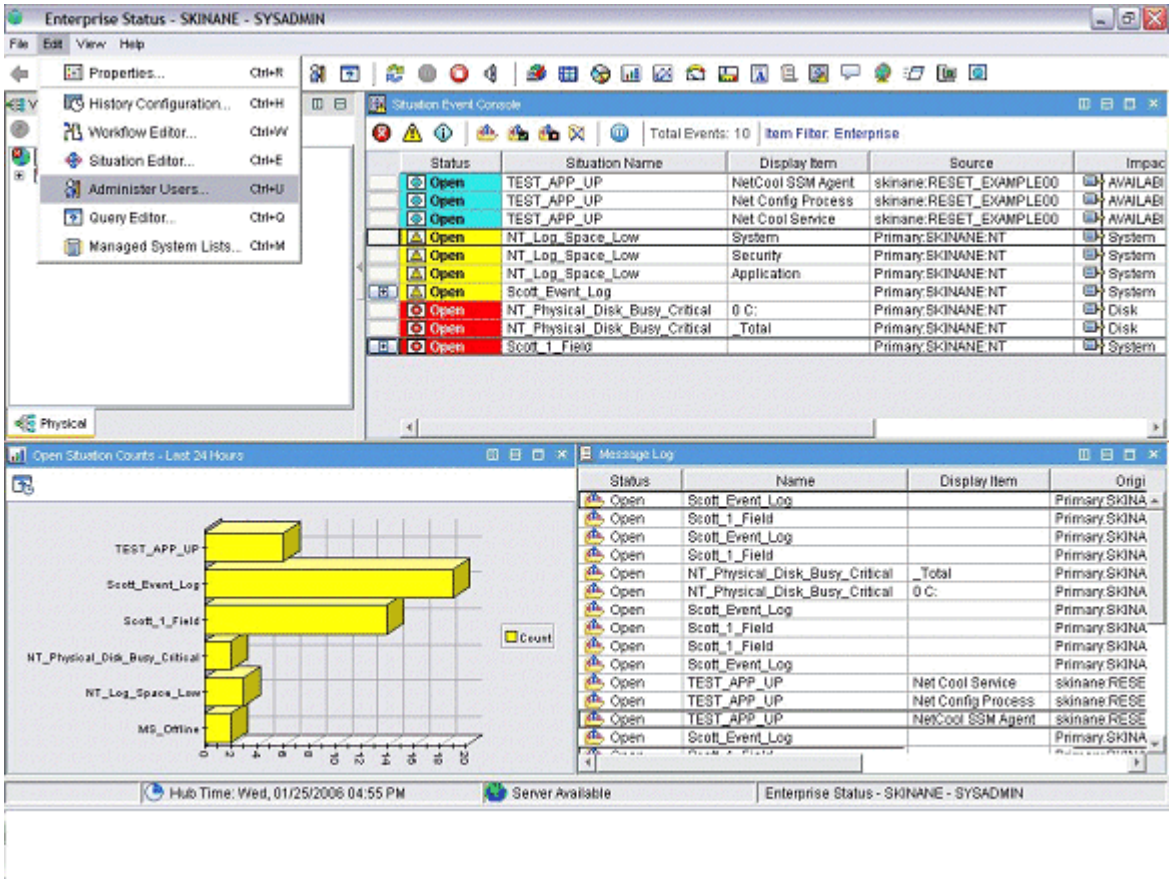


Figura 61. Establecimiento del ID de usuario `sysadmin`

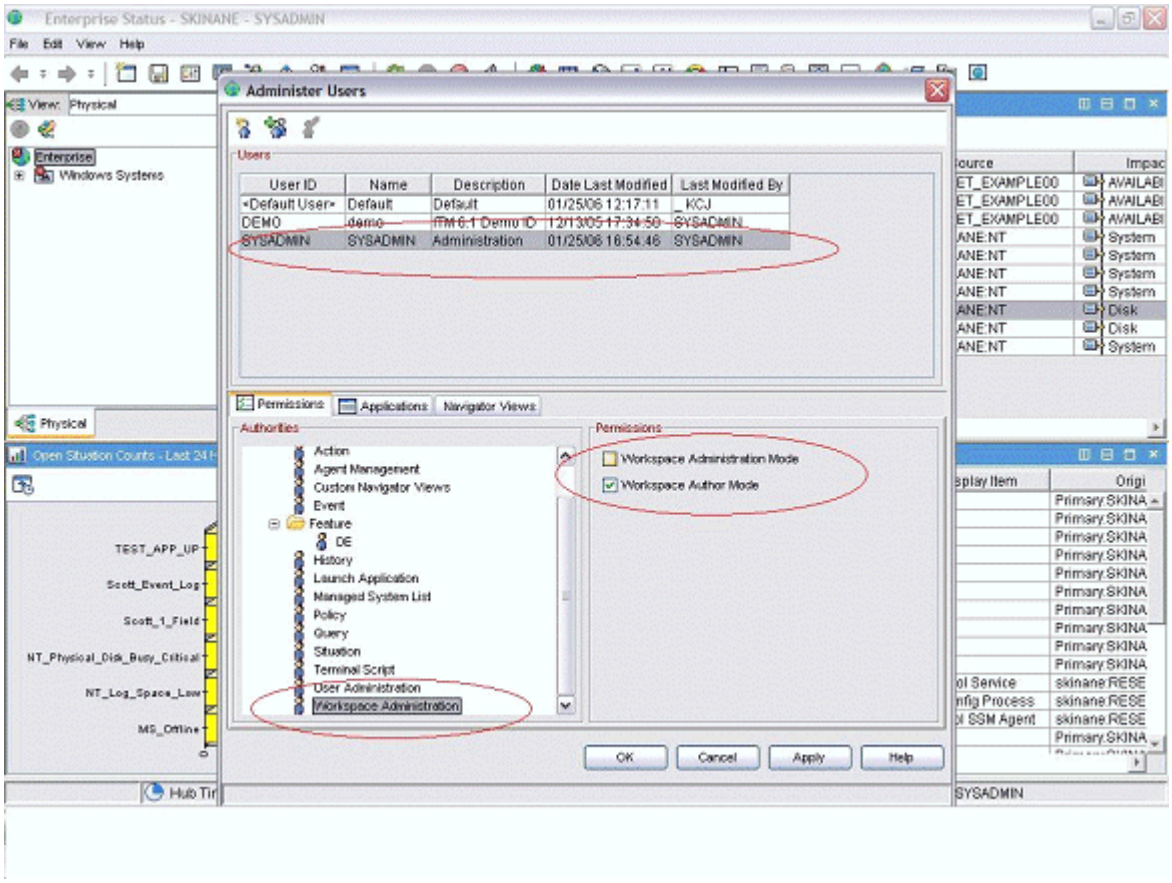


Figura 62. Establecimiento del ID de usuario `sysadmin` (continuación)

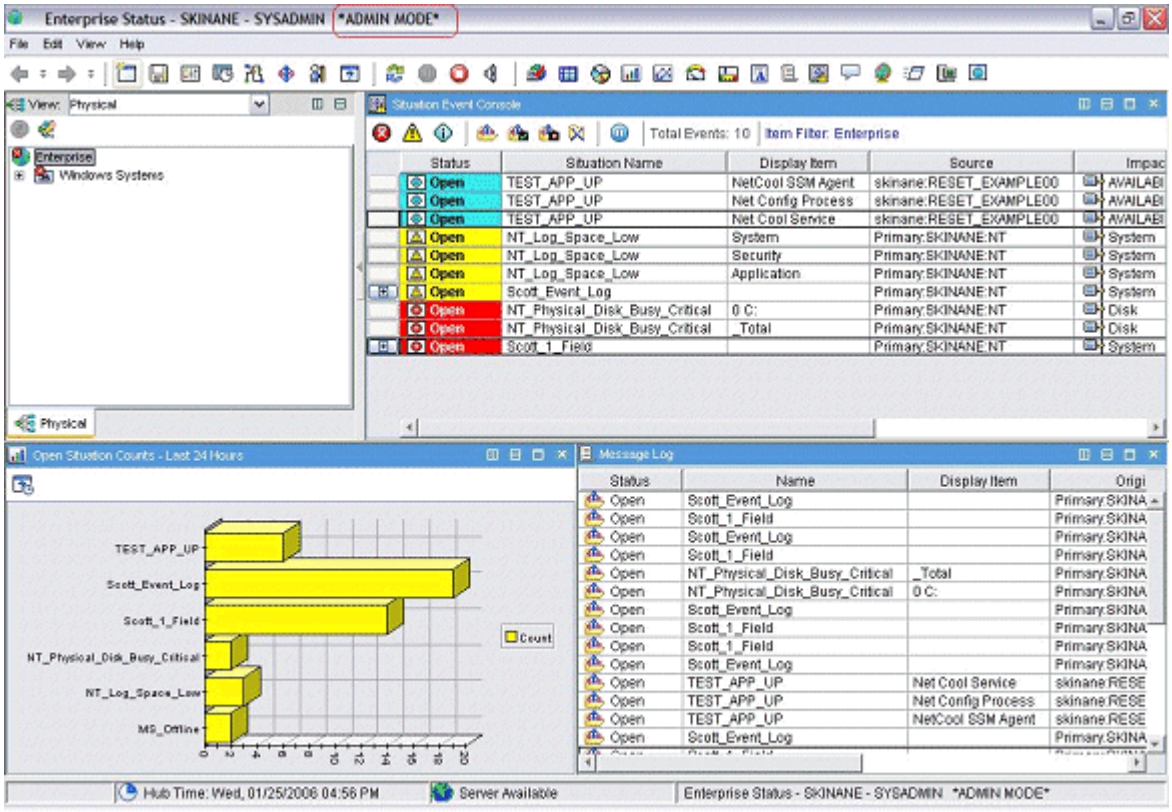


Figura 63. Establecimiento del ID de usuario `sysadmin` (continuación)

Qué hacer a continuación

Cuando esté en modalidad de "Administrador" tal como se representa en la Figura 63 en la página 1412, estará preparado para crear espacios de trabajo para la aplicación. Para obtener más información sobre cómo personalizar y crear espacios de trabajo, consulte la Guía del usuario de Tivoli Enterprise Portal. Como alternativa, utilice la documentación de ayuda que se instala con el componente Tivoli Enterprise Portal.

Si desea que los espacios de trabajo sean de "solo lectura" y que un cliente no los pueda suprimir, establezca las propiedades "no editable" y "no suprimible" para cada espacio de trabajo. En las propiedades de espacio de trabajo, seleccione las siguientes propiedades:

- **No permitir modificaciones**
- **Proporcionado por el producto de IBM (marcar como no suprimible)**

Puede ir a las propiedades visualizando un espacio de trabajo o pulsando el icono con los controles que se encuentran en él. También puede ir a una de las páginas de propiedades de vista y luego al nivel de espacio de trabajo en propertTambtree. Si tiene más de un espacio de trabajo para cada elemento de Navigator, recuerde establecer las propiedades de cada espacio de trabajo. Como se indica en la siguiente captura de pantalla de ejemplo:

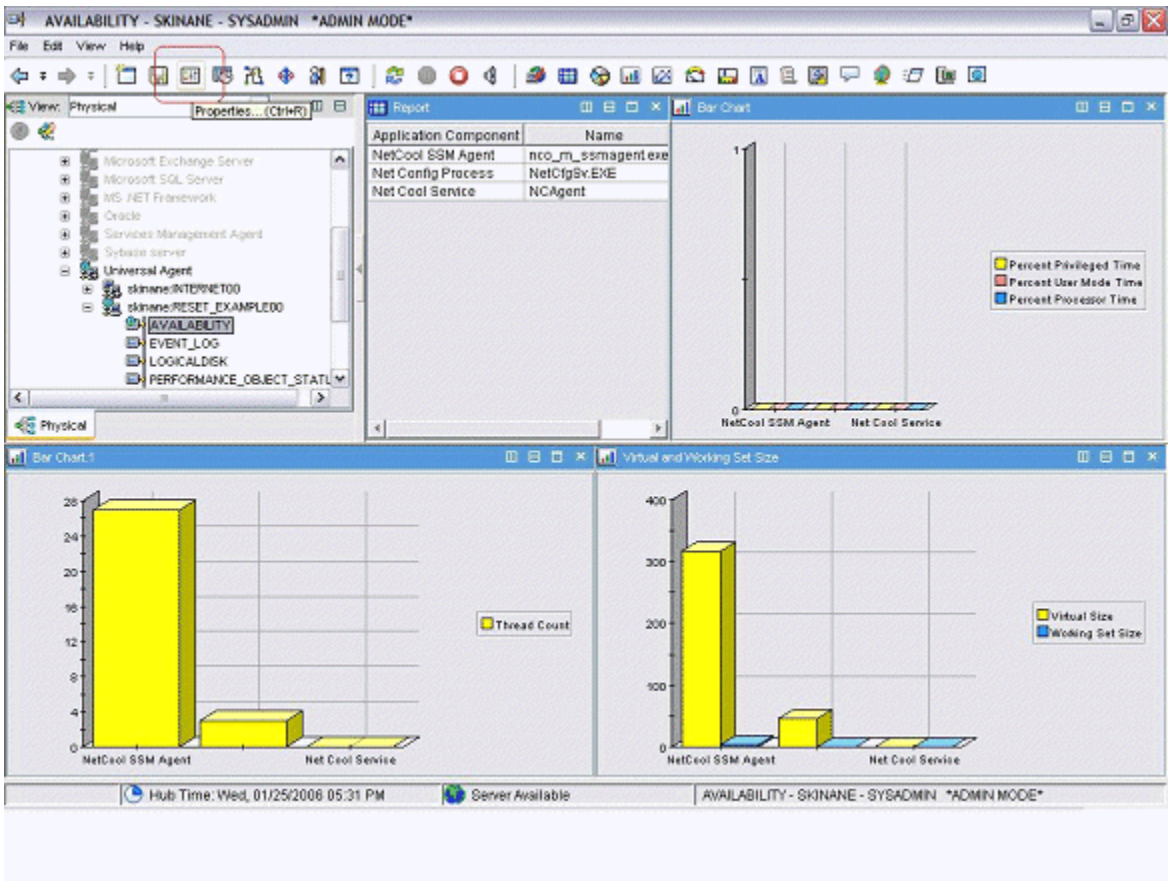


Figura 64. Establecer propiedades de espacios de trabajo

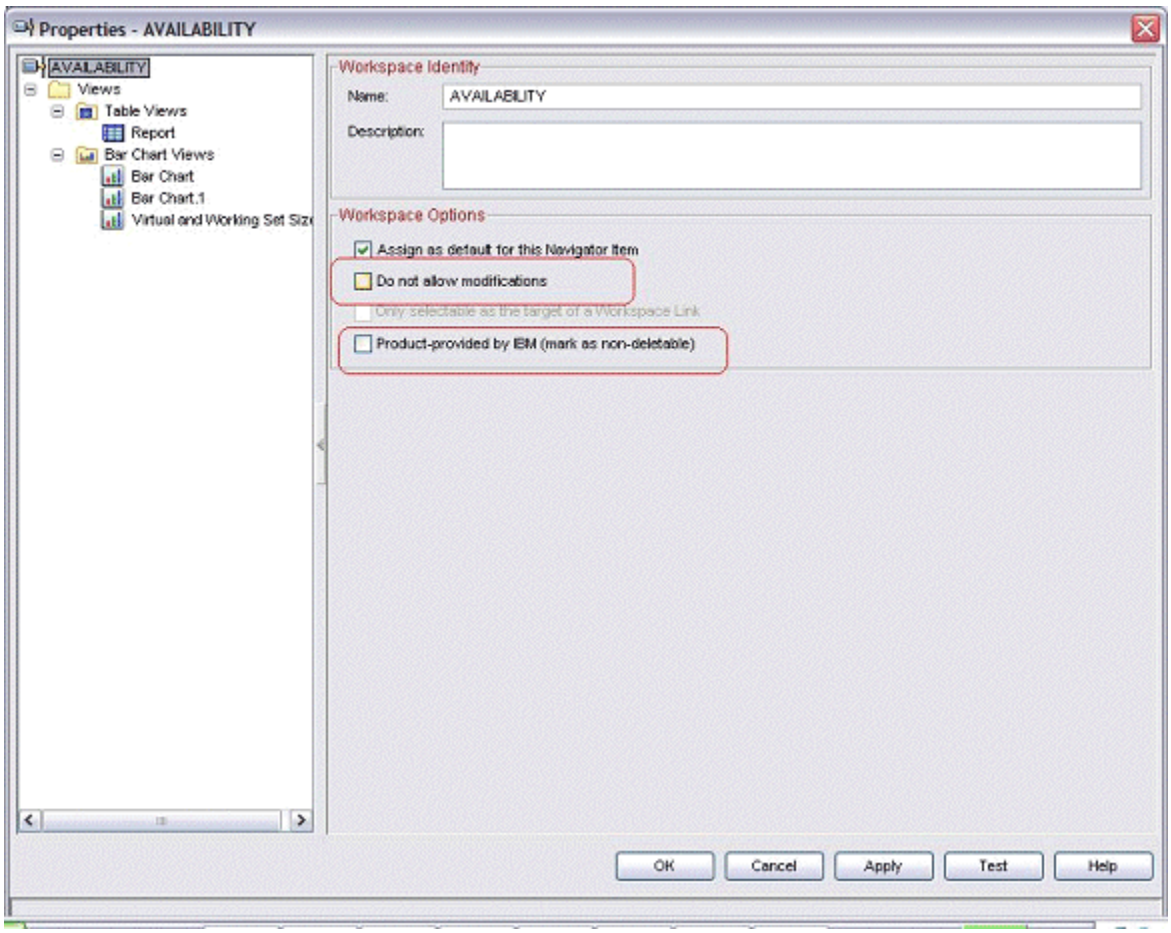


Figura 65. Establecer propiedades de espacios de trabajo (continuación)

Preparación del agente para Cloud APM

Si desea utilizar el agente con IBM Cloud Application Performance Management, tendrá que prepararlo mediante el asistente de **Configuración de panel de instrumentos**. Este asistente configura la información que puede ver en los paneles de instrumentos de detalles y resumen en Cloud APM. También establece la información de recurso que Cloud APM necesita para el agente.

Antes de empezar

Para preparar el agente para Cloud APM satisfactoriamente, debe asegurarse de que el agente proporciona los datos siguientes:

- Uno o varios conjuntos de datos (grupos de atributos) que producen una fila de datos. Puede utilizar los atributos de estos conjuntos de datos para llenar el panel de instrumentos de resumen.

  Importante: Para incluir cualquier información en el panel de instrumentos de resumen, debe proporcionarla en un conjunto de datos que genere una única fila de datos. Algunos orígenes de datos crean conjuntos de datos que generan varias filas de datos; por ejemplo, los orígenes de datos de proceso, servicio Windows, y código de retorno de mandato colocan datos en el único conjunto de datos de Disponibilidad, que genera varias filas. En estos casos, debe crear un conjunto de datos filtrado que produzca una fila para incluir los datos en un panel de instrumentos de resumen. Si desea más instrucciones, consulte “Creación de un grupo de atributos filtrado” en la página 1382.
- Un atributo numérico dentro de uno de estos conjuntos de datos que indica el estado del servicio supervisado (normal, aviso, crítico u otros valores de estado similares). Debe definir los valores de gravedad de estado para este atributo. Encontrará instrucciones sobre cómo definir los valores de

gravedad de estado en: “Especificar la gravedad de un atributo utilizado como indicador de estado” en la página 1238.

- Si el número de puerto en que la aplicación supervisada proporciona servicio es fijo, debe conocer el puerto. Si el puerto podría cambiar entre despliegues distintos, uno de los conjuntos de datos que producen una fila de datos debe contener un campo numérico que indique el puerto.
- Si se puede instalar el agente en un host para supervisar un servidor que se ejecuta en otro host, un atributo de serie dentro de uno de estos conjuntos de datos que indica la dirección IP del servidor. Si el agente supervisa siempre el host donde se ejecuta, tal atributo no es necesario.

  Consejo: Si está disponible un atributo que proporciona el nombre de host, puede crear un atributo derivado para la dirección IP mediante la función `nameToIpAddress`. Si desea más información sobre cómo crear un atributo derivado, consulte “Creación de atributos derivados” en la página 1231. Para obtener información sobre la función, consulte “ipAddressToName” en la página 1245.

Si el agente tiene subnodos, estos requisitos se aplican a cada subnodo para el que desea crear un panel de instrumentos.

Acerca de esta tarea

Cloud APM supervisa *recursos*. Un recurso corresponde a instancia del agente, o algunas veces un subnodo. Para definir un recurso, debe suministrar un nombre de tipo de recurso, un nombre de servidor, una dirección IP y un número de puerto que se aplican al servicio supervisado.

Cloud APM muestra un panel de instrumentos de resumen para cada recurso supervisado. El panel de instrumentos de resumen incluye un indicador de estado; con este indicador (normalmente verde, amarillo o rojo para estado normal, de aviso o crítico) el usuario puede ver el estado del recurso a simple vista. El mismo panel de instrumentos puede contener otras pocas métricas de estado de alto nivel.

En el panel de instrumentos de resumen, los datos se muestran como elementos únicos. Por lo tanto, el conjunto de datos con estos datos debe producir solo una fila.

De forma opcional, puede estar disponible un panel de instrumentos de detalles para el agente. El usuario puede pulsar el panel de instrumentos de resumen para ver el panel de instrumentos de detalles. El panel de instrumentos de detalle puede visualizar tablas, de modo que los datos de cualquier conjunto de datos se puedan utilizar en este panel de instrumentos.

Debe seleccionar los atributos que se muestran en el panel de instrumentos de resumen (incluido el indicador de estado) y en el panel de instrumentos de detalles.

Importante: Los datos de los atributos que selecciona se pasan automáticamente del agente al servidor de Cloud APM cada minuto. Si se especifican demasiados datos puede llevar a la sobrecarga de la red, el servidor o el host supervisado. Seleccione los atributos necesarios solo. Por ejemplo, si se debe mostrar un conjunto de datos unido o un atributo derivado, no especifique los atributos de origen también.

Importante: No se pasa ningún dato más que estos atributos a Cloud APM. No puede ver o utilizar otros datos en Cloud APM, excepto para los umbrales, que se supervisan en el nivel de agente. Si utiliza otros datos en umbrales, quizá no pueda ver el estado de umbral en la consola de Cloud APM.

Procedimiento

1. En la vista **Información de agente**, pulse el enlace **Paneles de instrumentos**.
2. En **Componentes de paneles de instrumentos**, seleccione **Mostrar componentes de agente en el panel de instrumentos**.

   Consejo: De forma alternativa, si está creando un agente para utilizar exclusivamente con IBM Tivoli Monitoring, puede seleccionar **No existe un panel de instrumentos para este agente**. En este caso, no realice los pasos posteriores de este procedimiento. No se puede instalar un agente así en un entorno de Cloud APM.
3. Pulse el enlace **Asistente de configuración del panel de instrumentos**.
4. Si el agente tiene subnodos, defina la disposición de recursos de agente y subnodo en Cloud APM:

- Seleccione **Instancias de agente base** para visualizar el agente base (datos fuera de subnodos) como un recurso.
- Para cada subnodo, seleccione **Instancias de subnodo "*nombre*"** para visualizar este subnodo como un recurso.
- De forma opcional, para cualquiera de los subnodos seleccionados, seleccione **Mostrar como hijo de agente**. En este caso, el recurso de subnodo se visualiza como un hijo bajo el recurso de agente en listas en la consola de Cloud APM.

Cloud APM muestra un panel de instrumentos de detalles y resumen para cada uno de los componentes seleccionados.

Importante: Si ejecuta el asistente y anula selección de un agente o un subnodo, los recursos del agente o subnodo no se eliminan automáticamente. Para eliminar los recursos, expanda **Recursos** en la vista esquema, seleccione los recursos que se van a suprimir y pulse la tecla Supr en el teclado.

5. En la página **Selección de atributo: Estado**, seleccione el atributo que indica el estado del servicio supervisado. Están disponibles atributos numéricos de grupos que devuelven una fila única de datos.

   Consejo: De forma alternativa, si no desea visualizar el estado en el panel de instrumentos, deseleccione **Proporcionar estado para este agente**.
6. En la misma página, puede seleccionar si desea mostrar datos adicionales en los paneles de instrumentos de detalles y resumen:
   - Para mostrar métricas de estado de alto nivel adicionales en el panel de instrumentos de resumen, asegúrese de que está seleccionado el recuadro **Seleccionar atributos adicionales a mostrar en esta información de resumen de agente**. De lo contrario, borre el recuadro.
   - Para mostrar datos adicionales en el panel de instrumentos de detalles, asegúrese de que está seleccionado el recuadro **Seleccionar los atributos adicionales que se mostrarán en esta información de detalles del agente**. De lo contrario, borre el recuadro. (Normalmente, seleccione este recuadro, porque es necesario un panel de instrumentos de detalles para mostrar datos suficientes para que sea significativo un agente de supervisión).

   Pulse **Siguiente**.
7. Si ha seleccionado **Seleccionar atributos adicionales a mostrar en esta información de resumen de agente**, en la página **Selección de atributo: Resumen**, seleccione hasta cuatro atributos adicionales para incluirlos en el panel de instrumentos de resumen. Están disponibles atributos de grupos que devuelven una sola fila de datos. Pulse **Siguiente**.
8. Si ha seleccionado **Seleccionar los atributos adicionales que se mostrarán en esta información de detalles del agente**, en la página **Selección de atributo: Detalles**, seleccione los atributos para incluirlos en el panel de instrumentos de detalles. Todos los atributos del agente están disponibles; para evitar problemas de rendimiento, incluya el menor número posible de atributos. Pulse **Siguiente**.
9. En la página **Tipo de recurso**, entre el tipo de servidor que está supervisando, por ejemplo, `Servidor de correo electrónico` o `Servidor de la base de datos SampleCo`. Pulse **Siguiente**.
10. En la página **Selección de atributo: Nombre del servidor de software**, especifique un nombre de servidor de software fijo en el campo **Nombre fijo** o seleccione un atributo en el agente que proporciona el nombre del servidor de software. Este nombre se muestra al usuario para esta instancia supervisada particular, por ejemplo, el nombre de la instancia del servidor de aplicaciones JBoss. Pulse **Siguiente**.

    Importante: No ejecute dos o más agentes de supervisión, instancias de agente o subnodos con el mismo nombre de servidor de software en el mismo host supervisado. Si el agente tiene instancias o subnodos, asegúrese de que se genera un único nombre de servidor de software para cada instancia o subnodo. Si dos agentes distintos producen el mismo nombre de servidor de software, no los instale en el mismo host supervisado.
11. En la página **Selección de atributo: dirección IP**, seleccione un atributo en el agente que especifique la dirección IP (no el nombre de host) de la conexión de interfaz principal que utiliza la aplicación o el servidor supervisado. Por ejemplo, la conexión HTTP para un servidor HTTP o la conexión del cliente

de base de datos para un servidor de bases de datos. O bien, seleccione **Utilizar la dirección IP del agente** para utilizar la dirección del host donde se ejecuta el agente. Pulse **Siguiente**.

12. En la página **Selección de atributo - Puerto**, especifique el puerto en que la aplicación supervisada proporciona servicio o seleccione un atributo numérico en el agente que especifique este puerto. Pulse **Finalizar**.
13. Si ha seleccionado un agente y un subnodo o más de un subnodo como recursos, pulse **Siguiente** para especificar información de panel de instrumentos y recurso para el siguiente componente (agente o subnodo). Si el botón **Siguiente** está inhabilitado, ha especificado la información para todos los componentes necesarios; pulse **Finalizar** para completar el asistente.

Resultados
Al instalar el agente en un host supervisado, puede ver los paneles de instrumentos de resumen y de detalle en la pestaña **Visión general de estado**.

Importante: Puede haber un retardo de hasta 30 minutos entre la instalación del agente y la disponibilidad de los paneles de instrumentos, especialmente si esta es la primera vez que se ha instalado este tipo de agente y esta versión en su entorno.

Pulse el panel de instrumentos de resumen para el agente para ver el panel de instrumentos de detalles. De forma predeterminada, toda la información del panel de instrumentos de detalles se mostrará como tablas.

Puede utilizar la pestaña **Detalles de atributo** para configurar la visualización personalizada de esta información como tablas y gráficos.

Pruebas del agente en Agent Builder

Después de utilizar Agent Builder para crear un agente, puede probarlo en Agent Builder.

Pruebe el agente para garantizar que los datos de supervisión que espera son los datos que se visualizan. Mediante la prueba del agente, puede aprender a modificar o retocar los valores en el agente para asegurar que los datos mostrados sean útiles y precisos.

Puede probar el agente en Agent Builder utilizando los métodos siguientes:

1. Comience a utilizar la función de prueba de grupo de atributos de Agent Builder para probar grupos de atributos individuales uno a uno. Para obtener más información, consulte “Prueba de grupo de atributos” en la página 1417.
2. Después de completar la prueba de grupo de atributos, puede utilizar la función prueba de agente de Agent Builder para probar todos los grupos de atributos en el agente a la vez. Para obtener más información, consulte “Prueba de todo el agente” en la página 1421.

Importante: Al probar el agente en Agent Builder, podrá ver los valores especiales siguientes para atributos numéricos:

- -1: un error general
- -2: datos que faltan
- -3: ningún valor (por ejemplo, una base de datos ha devuelto NULL)

Prueba de grupo de atributos

Puede utilizar la prueba de grupo de atributos del agente para probar los grupos de atributo que creó con Agent Builder, un grupo de atributos a la vez. Puede probar varios grupos de atributo antes de completar la definición de grupo de atributos. Por ejemplo, puede iniciar la prueba desde el **Asistente de Agente de IBM Tivoli Monitoring** cuando defina los grupos de atributo de un agente nuevo. Puede también iniciar la prueba desde el **Asistente de Componente de agente de IBM Tivoli Monitoring** cuando añada los grupos de atributo a un agente existente.

Antes de empezar

Antes de empezar a probar un grupo de atributos, puede, opcionalmente:

- Definir las preferencias de prueba del grupo de atributos. Para obtener más información, consulte "Prueba de grupo de atributos - preferencias" en la página 1419.
- Definir variables de entorno, propiedades de configuración y, donde corresponda, información de Java. Para obtener más información, consulte "Prueba de grupo de atributos - configuración" en la página 1420.

Acerca de esta tarea

Agent Builder da soporte a una función de prueba de grupo de atributos para la mayoría de los orígenes de datos

Procedimiento

- Inicie el procedimiento de prueba de las siguientes formas:
  1. Durante la creación del agente o grupo de atributos pulse **Probar** en la página Información importante de origen de datos.
  2. Después de la creación del agente, seleccione un grupo de atributos en la página **Definición de origen de datos** de Agent Editor y pulse **Probar**. Para obtener más información sobre Agent Editor, consulte "Utilización del editor del agente para modificar el agente" en la página 1208.

  Después de pulsar **Probar** en uno de los dos pasos anteriores, se visualiza la ventana Prueba de grupo de atributos. Esta ventana es diferente para distintos orígenes de datos.

  Agent Builder da soporte a una función de prueba de grupo de atributos para la mayoría de los orígenes de datos.

  Para obtener más información sobre los procedimientos de pruebas para grupos de atributos específicos, consulte las siguientes secciones de pruebas:

  – Windows Management Instrumentation (WMI), para obtener más información sobre el procedimiento de prueba de WMI, consulte "Prueba de grupos de atributos de WMI" en la página 1264
  – Windows Performance Monitor (Perfmon), para obtener más información acerca del procedimiento de prueba de Perfmon, consulte "Prueba de grupos de atributos de Perfmon" en la página 1266
  – Simple Network Management Protocol (SNMP), para obtener más información sobre la prueba de SNMP, consulte "Prueba de grupos de atributos SNMP" en la página 1271
  – Remitente de sucesos Simple Network Management Protocol (SNMP), para obtener más información sobre el procedimiento de pruebas de sucesos de SNMP, consulte "Prueba de grupos de atributos de sucesos de SNMP" en la página 1276
  – Java Management Extensions (JMX), para obtener más información acerca del procedimiento de prueba de JMX, consulte "Prueba de grupos de atributos de JMX" en la página 1296
  – Common Information Model (CIM), para obtener más información sobre el procedimiento de pruebas de CIM, consulte "Prueba de grupos de atributos de CIM" en la página 1299
  – Archivo de registro, para obtener más información sobre el procedimiento de pruebas del archivo de registro, consulte "Prueba de grupos de atributos de archivo de registro" en la página 1310
  – Script, para obtener más información sobre el procedimiento de prueba de script, consulte "Pasos para supervisar la salida de un script" en la página 1321
  – Java Database Connectivity (JDBC), para obtener más información acerca del procedimiento de prueba de JDBC, consulte "Prueba de grupos de atributos JDBC" en la página 1332
  – Ping de Internet Control Message Protocol (ICMP), para obtener más información sobre el procedimiento de pruebas de ICMP, consulte "Prueba de grupos de atributos de ping" en la página 1334

- Disponibilidad de Hypertext Transfer Protocol (HTTP), para obtener más información sobre el procedimiento de pruebas de HTTP, consulte "Prueba de grupos de atributos de HTTP" en la página 1343
- SOAP, para obtener más información sobre el procedimiento de prueba de SOAP, consulte "Prueba de grupos de atributos de SOAP" en la página 1351
- Socket Transmission Control Protocol socket (TCP), para obtener más información sobre el procedimiento de pruebas de socket, consulte "Prueba de grupos de atributos de socket" en la página 1362
- Java application programming interface (API), para obtener más información acerca del procedimiento de prueba de la API de Java, consulte "Prueba de grupos de atributos de aplicación Java" en la página 1376

Algunos orígenes de datos no tienen una función de prueba de grupo de atributos, por ejemplo:

- Cuando puede utilizar el navegador de Agent Builder para visualizar datos activos en un sistema. Por ejemplo, puede ver los procesos que están ejecutándose actualmente en el sistema (procesos). Otros ejemplos son cuando visualiza los servicios que están instalados en el sistema (servicios de Windows) y los registros de sucesos de Windows presentes.
- Puede realizar muy poca personalización en el agente (AIX Binary Log, código de retorno de mandato).
- Los grupos de atributo unidos o filtrados no pueden probarse mediante la función de prueba de grupo de atributos ya que estos se basan en varios grupos de atributos.

Nota:

1. Utilice la prueba completa del agente para probar orígenes de datos que no se pueden probar utilizando la función de prueba de grupo de atributos. Si desea más información sobre la prueba completa del agente, consulte "Prueba de todo el agente" en la página 1421.
2. Cuando pruebe los orígenes de datos, después de pulsar **Recopilar datos**, los datos podrían no mostrarse o podrían no ser actuales después de la primera pulsación. En tales casos, pulse **Recopilar datos** por segunda vez para visualizar los datos actuales.

- Depuración:

  Cada origen de datos que se prueba tiene un directorio de prueba que Agent Builder ha creado para él. Este directorio se utiliza para el entorno de ejecución de prueba del origen de datos. Los archivos de registro que se relacionan con las pruebas que se ejecutan en el origen de datos se almacenan bajo este directorio. Los archivos de registro pueden ser útiles para resolver problemas de depuración que se encuentran durante la prueba.

  Nota:

  1. La ubicación del archivo de registro de prueba se muestra como un mensaje de estado en la ventana **Probar** después de pulsar **Iniciar agente** y también después de pulsar **Detener agente**.
  2. Todos los directorios del origen de datos de prueba se suprimen cuando Agent Builder se cierra.

Prueba de grupo de atributos - preferencias
Establezca las preferencias antes de probar un grupo de atributos.

Acerca de esta tarea
Antes de iniciar la prueba de un grupo de atributos, puede establecer, de forma opcional, algunas preferencias que determinen cómo se tratarán los atributos durante la prueba.

Procedimiento

1. Seleccione **Ventana** > **Preferencias** en la barra de menús de Agent Builder.
   Se abrirá la ventana **Preferencias**.
2. Seleccione **Agent Builder**.
   Se mostrarán las preferencias asociadas con los grupos de atributos de prueba:

Diálogo Mostrar tipos de datos cambiados al realizar la prueba
Cuando está seleccionada, Agent Builder sugiere los cambios del tipo de datos de un atributo. Agent Builder sugiere cambios cuando el tipo de datos de un atributo no coincide con los datos devueltos por una prueba para ese atributo. Por ejemplo, si la longitud de la serie definida para un atributo es demasiado corta para contener un valor devuelto por una prueba. En este ejemplo, Agent builder sugiere redefinir el atributo para que tenga una longitud de serie mayor. Cuando esta opción no está seleccionada, Agent Builder no comprueba ni sugiere tipos de datos durante la prueba. Esta opción está seleccionada de forma predeterminada.

Número máximo de atributos de registro o script creados
El valor especificado en este campo determina el número máximo de atributos que analiza Agent Builder durante la prueba inicial de un grupo de atributos de script o archivo de registro. El valor predeterminado es 25.

3. Cuando haya terminado de establecer sus preferencias, pulse **Aceptar** para guardar sus valores y cierre la ventana **Preferencias**.

   Si desea restaurar los valores predeterminados, pulse **Restaurar valores predeterminados** antes de pulsar **Aceptar**

Prueba de grupo de atributos - configuración
Antes de iniciar la prueba, establezca las variables de entorno, las propiedades de configuración y la información de Java.

Acerca de esta tarea
Antes de iniciar la prueba de un grupo de atributos, puede establecer, de forma opcional, las variables de entorno, las propiedades de configuración y, donde corresponda, la información de Java desde la ventana Prueba del origen de datos. La información Java es un subconjunto de los datos de configuración. Algunas variables de entorno tienen valores especiales definidos de forma predeterminada para la prueba de grupo de atributos. Para obtener más información acerca de las variables de entorno con valores especiales para la prueba del grupo de atributos, consulte “Variables de entorno de prueba” en la página 1425.

Procedimiento

1. Opcional: Pulse **Establecer entorno** en la ventana **Probar** del origen de datos.
   Se abrirá la ventana **Variables de entorno**. Cuando se llena, la ventana **Variables de entorno** lista todas las variables de entorno que se utilizan durante la ejecución de la prueba. La vista inicial de la ventana Variable de entorno contiene las variables de entorno existentes que ha definido en el agente. También contiene las variables de entorno que ha añadido en pruebas anteriores de este agente.
   a) Pulse **Añadir** o **Editar** para añadir o editar variables individuales.
   b) Pulse **Eliminar** para eliminar variables individuales, o **Restaurar valores predeterminados** para restaurar las variables predeterminadas y eliminar todas las otras.
   c) Pulse **Aceptar** para guardar los cambios y volver a la ventana **Probar**.
2. Opcional: Pulse **Configuración** en la ventana **Probar** del origen de datos. Se abrirá la ventana **Configuración de tiempo de ejecución**.
   a) Pulse **Editar configuración de agente** para añadir una propiedad de configuración o para editar las propiedades de configuración de agente existentes mediante la ventana **Propiedades de configuración**.
   b) Seleccione un propiedad de configuración y pulse **Editar** para editar una propiedad de configuración existente relacionada al grupo de atributo que está probando.
   c) Seleccione un propiedad de configuración y pulse **Restaurar predeterminado** para restaurar la propiedad de configuración a su valor predeterminado.

   Importante: Si un origen de datos JMX se conecta a un WebSphere Application Server remoto, asegúrese de que hay instalado un WebSphere Application Server local y que la ubicación de Java está establecida en el JRE que utiliza este servidor. Para obtener más detalles sobre cómo establecer la conexión, consulte “Supervisión de MBeans Java Management Extensions (JMX)” en la página 1278.

3. Pulse **Aceptar** para guardar los cambios y volver a la ventana **Probar**.
4. **Nota:** Puede establecer información de Java para los siguientes tipos de grupos de atributos:
   - Java Management Extensions (JMX)
   - Java Database Connectivity (JDBC)
   - Disponibilidad de Hypertext Transfer Protocol (HTTP)
   - SOAP
   - Interfaz de programación de aplicación (API) Java

   La información de Java es un subconjunto de los datos de configuración descritos en el paso "2" en la página 1420

   Opcional: Pulse **Información de Java** en la ventana **Probar** del origen de datos.

   Se abrirá la ventana **Information de java**.

   a) Especifique la información de Java.
   Por ejemplo, vaya a, o especifique, la ubicación de Java Runtime Environment (JRE), seleccione un **Nivel de rastreo de Java** o especifique **Argumentos de JVM**

   b) Pulse **Aceptar** para guardar los cambios y volver a la ventana **Probar**.

Prueba de todo el agente

Utilice la prueba de todo el agente para probar todos los grupos de atributos del agente. También puede utilizar la prueba de todo el agente para probar orígenes de datos que no pueden probarse utilizando la función de prueba del grupo de atributos.

Acerca de esta tarea

Puede utilizar la prueba de todo el agente para ejecutar el agente de la misma manera que se ejecuta en IBM Tivoli Monitoring sin necesidad de una instalación de IBM Tivoli Monitoring.

Importante: En sistemas Windows, si desea ejecutar una prueba completa del agente dentro de Agent Builder (consulte "Prueba de todo el agente" en la página 1421), asegúrese de que, en la ventana de información del agente, está seleccionada la versión de 32 bits del sistema operativo en el cual está ejecutando Agent Builder, es decir, Windows de 32 bits. En sistemas Linux, debe estar seleccionada la versión de 64 bits.

Procedimiento

1. Abra la perspectiva **Prueba de agente**:
   a) En Agent Editor, abra el separador **Información de agente**.
   b) Pulse **Probar el agente**.

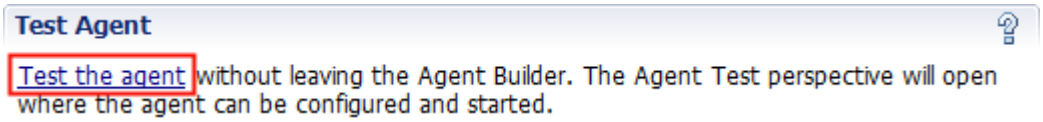


*Figura 66. Sección **Probar agente** de **Agent Editor**, página **Información de agente**.*

   De forma alternativa, en el menú de Agent Builder, seleccione **Ventana** > **Abrir perspectiva** > **Otro**, seleccione **Prueba de agente** y pulse **Aceptar**

Se abre la perspectiva **Prueba de agente** (Figura 68 en la página 1424). La vista **Prueba del agente** muestra agentes que ha abierto en el editor de agentes; puede probar cualquiera de estos agentes. También se visualiza la vista **Prueba de grupo de atributos**; esta vista está vacía inicialmente. La vista **Prueba de grupo de atributos** muestra datos que se recopilan de un grupo de atributos seleccionado cuando se ejecuta el agente.

Consejo: Si no se edita ningún agente, la perspectiva **Prueba de agente** está vacía. Para llenar la vista, vaya a la perspectiva **IBM Tivoli Monitoring** y abra un agente en **Agent Editor**. Cuando se abre un agente en **Agent Editor**, vuelve a la perspectiva **Prueba de agente** para probar el agente.

2. Opcional: Configure las variables de entorno y las propiedades de configuración antes de iniciar la prueba.

   Puede acceder a las ventanas **Variables de entorno** y **Configuración de tiempo de ejecución** de dos maneras desde la vista **Prueba de agente**:

   - Pulse con el botón derecho del ratón en el agente en la vista **Prueba de agente** para abrir un menú de selección. Puede seleccionar **Establecer entorno** en el menú para abrir la ventana **Variables de entorno**. Puede seleccionar **Configuración** en el menú para abrir la ventana **Configuración de tiempo de ejecución**.
   - Pulse el icono de menú de vista en la barra de herramientas de la vista de **Agent Test** para acceder a los elementos de menú **Establecer entorno** y **Configuración** como en la opción anterior.

   Para obtener más información sobre la utilización de las ventanas **Variables de entorno** y **Configuración de tiempo de ejecución**, consulte "Prueba de grupo de atributos" en la página 1417.

   Importante:

   a. El agente se llena automáticamente con el último conjunto de configuración que está relacionado con cada grupo de atributos probados.

   b. Algunas variables de entorno pueden tener diferentes valores predeterminados para la prueba de grupos de atributos y para la prueba de todo el agente. Para obtener más información sobre las variables de entorno con valores especiales para la prueba de grupos de atributos, consulte "Variables de entorno de prueba" en la página 1425.

   c. Si un origen de datos JMX se conecta a un WebSphere Application Server remoto, asegúrese de que hay instalado un WebSphere Application Server local y que la ubicación de Java está establecida en el JRE que utiliza este servidor. Para obtener más detalles sobre cómo establecer la conexión, consulte "Supervisión de MBeans Java Management Extensions (JMX)" en la página 1278.

   d. En un origen de datos de API de Java, JDBC, JMX, HTTP o SOAP, puede utilizar los valores de **Java** > **Argumentos de JVM** para controlar el registro de rastreo de agente. Establezca el siguiente valor:

   ```
   -DJAVA_TRACE_MAX_FILES=archivos -DJAVA_TRACE_MAX_FILE_SIZE=tamaño
   ```

   donde *archivos* es la cantidad máxima de archivos de registro de rastreo que se guardan (el valor predeterminado es 4) y *tamaño* es el tamaño máximo del archivo de registro en kilobytes (el valor predeterminado es 5000). Por ejemplo, puede establecer el siguiente valor:

   ```
   -DJAVA_TRACE_MAX_FILES=7 -DJAVA_TRACE_MAX_FILE_SIZE=100
   ```

   En este caso, el agente graba 100 kilobytes en el primer archivo de registro y, a continuación, conmuta al segundo archivo de registro, y así sucesivamente. Después de grabar siete archivos de registro de 100 kilobytes cada uno, se graba encima del primer archivo de registro.

   e. Si el agente tiene subnodos, en una versión instalada puede establecer distintos valores de configuración para diferentes subnodos y de forma separada para los grupos de atributos del agente base. Sin embargo, en una configuración completa de prueba de agente, sólo puede establecer cada valor de configuración una vez; el valor se aplica al agente base y a los subnodos. Sólo puede probar una instancia de cada subnodo.

3. En la vista **Prueba del agente**, seleccione el agente que desea probar y pulse el icono  **Iniciar agente**.

   Una ventana indica que el agente se está iniciando. Cuando se inicia el gente, sus grupos de atributos se muestran como hijos del agente en la vista **Prueba de agente**. Los grupos de atributos se indican mediante el icono de grupo de atributos  .

Los grupos de atributos de estatus que ofrecen información sobre el agente (**Estatus de objeto de rendimiento**, **Estatus de agrupación de hebras** y **Estatus de actuación**) también se muestran como hijos del agente en la vista **Probar agente**. Los grupos de atributos de estatus se indican mediante el icono de información .

Puede iniciar y ejecutar más de un agente a la vez.

El icono **Detener agente** pasa a estar disponible cuando se inicia al agente.

Si el agente tiene subnodos o grupos de Navigator, se muestran como nodos en la ventana **Probar agente**. Las definiciones de subnodo se muestran bajo el agente. Un nodo de instancia de subnodo se muestra bajo el nodo de definición de subnodo. Los grupos de atributo y los grupos de navegador se muestran bajo el nodo de instancia de subnodo. Por ejemplo:

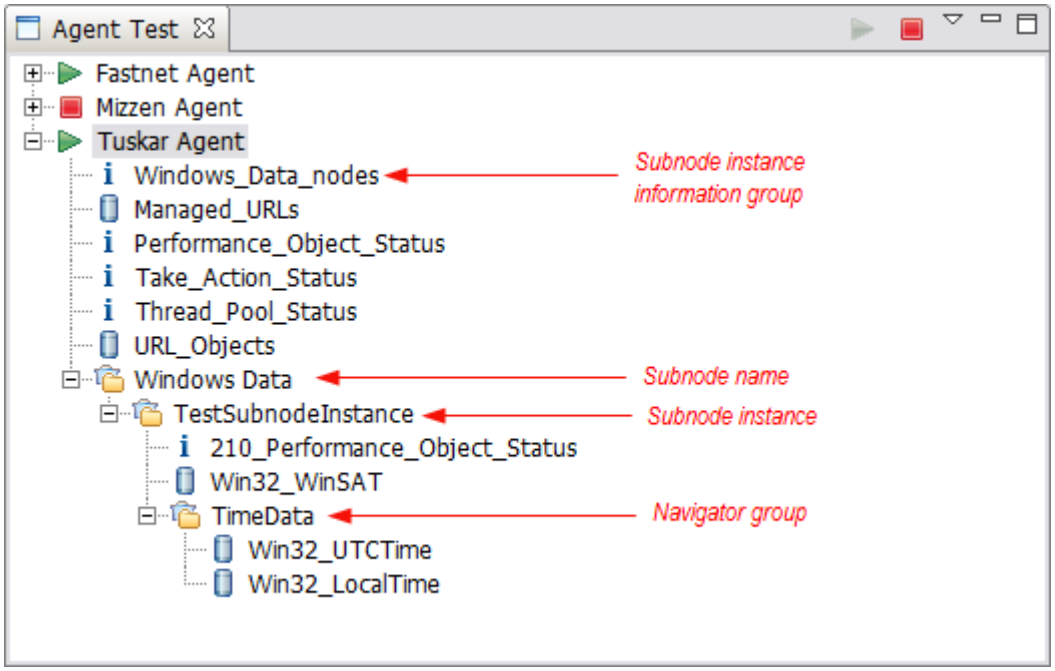


*Figura 67. Vista **Prueba de agente** con el subnodo y el grupo de Navigator de ejemplo resaltado.*

Puede pulsar con el botón derecho del ratón en cualquiera de los nodos de la vista **Prueba de agente** para acceder a las selecciones de menú como **Editar** y **Detener agente**. **Editar** abre **Definición de origen de datos** para el nodo seleccionado en **Agent Editor**.

Nota: Los cambios que realiza con **Agent Editor** no están visibles en el agente en ejecución hasta que detiene y reinicia el agente.

4. En la vista **Prueba de agente**, seleccione el primer grupo de atributos que desea probar.

   Al seleccionar un grupo de atributos, comienza una recopilación de datos para el grupo de atributos seleccionado. Si la recopilación tarda tiempo, una ventana indica que la recopilación de datos está en curso. Cuando se completa la recopilación de datos, los datos recopilados se visualizan en la vista **Prueba de grupo de atributos**, por ejemplo:

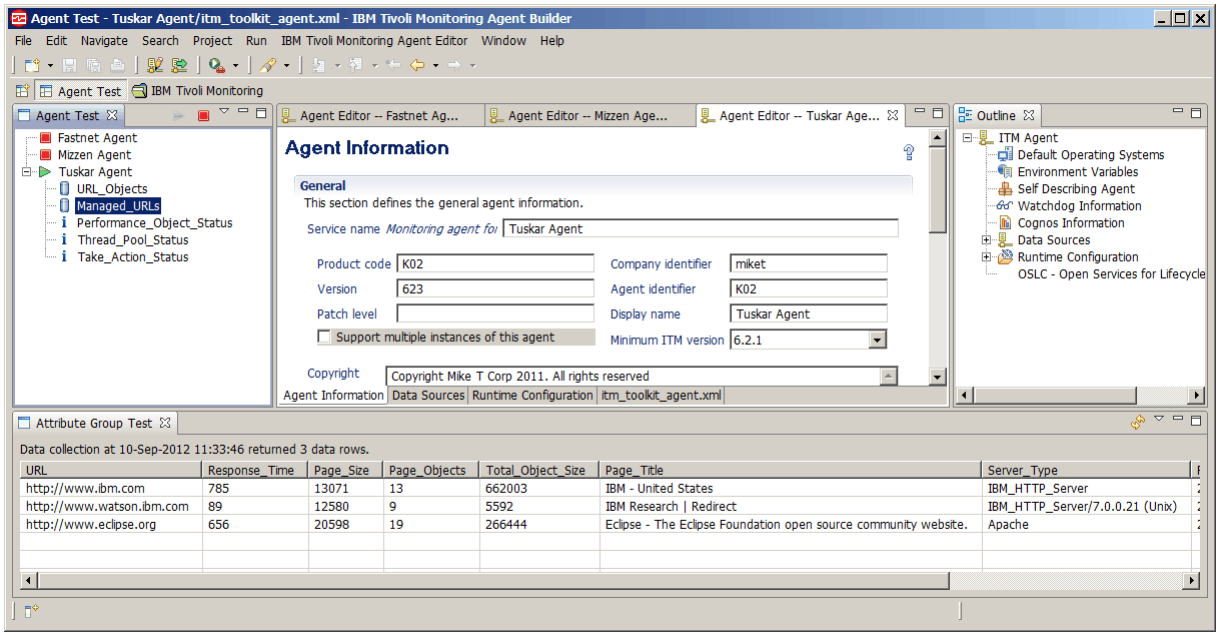


*Figura 68. Perspectiva **Prueba de agente***

Si no se visualiza ningún dato, se muestra el mensaje `Se han devuelto 0 filas de datos` en la vista **Prueba de grupo de atributos**. Hay varias razones por las que el agente puede no devolver datos. Las razones pueden ser:

- No hay datos
- Definición incorrecta
- Configuración incorrecta

Puede comprobar la razón por la que no se devuelven datos consultando el valor de **Error_Code** en el grupo de atributos **Estatus de objeto de rendimiento**. Para obtener más información sobre la visualización del grupo de atributos **Estatus de objeto de rendimiento**, consulte el paso “9” en la página 1425

Para recopilar datos de otro grupo de atributos del agente que se ejecuta, seleccione el grupo de atributos necesario.

Cuando selecciona un grupo de atributos en la vista **Prueba de agente**, el grupo de atributos correspondiente se visualiza en la vista **Agent Editor**.

5. Opcional: Ejecute una segunda recopilación de datos, después de la recopilación de datos inicial, para algunos tipos de grupos de atributos, para obtener valores de datos útiles.

   Para ejecutar una recopilación de datos, pulse el icono de recopilación de datos  en la vista **Prueba de grupo de atributos**.

   Si la recopilación tarda tiempo, una ventana indica que la recopilación de datos está en curso. Cuando se completa la recopilación de datos, los datos que se acaban de recopilar se visualizan en la vista **Prueba de grupo de atributos**.
6. Opcional: Pulse una cabecera de columna de atributos en la vista **Prueba de grupo de atributos** para abrir la **Información de atributos** en el separador **Definición de origen de datos** de **Agent Editor**. También puede acceder a la misma **Información de atributo** pulsando con el botón derecho del ratón en cualquier celda de la tabla y eligiendo **Editar** en el menú.

   Puede editar las propiedades del atributo en la forma normal. Los cambios que realice no están visible en el agente en ejecución hasta que detenga y reinicie el agente.
7. Opcional: Abra varias vistas **Prueba de grupo de atributos** a la vez.

Para abrir una vista **Prueba de grupo de atributos**, pulse el icono de menú de vista en la barra de herramientas de la vista **Prueba de grupo de atributos** y luego seleccione **Abrir vista para grupo de atributos**.

Nota: Cuando se abre la vista **Prueba de grupo de atributos**, se visualiza la misma información de atributos que la vista original **Prueba de grupo de atributos**. A continuación, puede seleccionar otro grupo de atributos en la vista **Prueba de agente** para visualizar información de otro grupo de atributos en la vista original **Prueba de grupo de atributos**. La primera vez que otra vista **Prueba de grupo de atributos** se abra, se abrirá en la misma ubicación que la vista original pero con su propio separador. Si desea ver las dos vistas simultáneamente, puede arrastrar el separador a otra ubicación en el espacio de trabajo.

8. Opcional: Seleccione el grupo de atributos de información de instancia de subnodo, si el agente tiene subnodos, para ver cómo se listan los subnodos en el agente (Figura 67 en la página 1423). La selección del grupo de atributos de información de instancia de subnodo muestra la información de instancia de subnodo en la vista **Prueba de grupo de atributos** (para todos los subnodos en línea del tipo seleccionado).
9. Opcional: Para obtener más información sobre la operación del agente, puede seleccionar los grupos de atributos **Estatus de objeto de rendimiento** y **Estatus de agrupación de hebras** en la vista **Prueba de agente**. Estos grupos de atributos de estatus se indican mediante el icono de información . Seleccione estos grupos para ver la información de estatus sobre las recopilaciones de datos anteriores para los grupos de atributos.

   Por ejemplo:

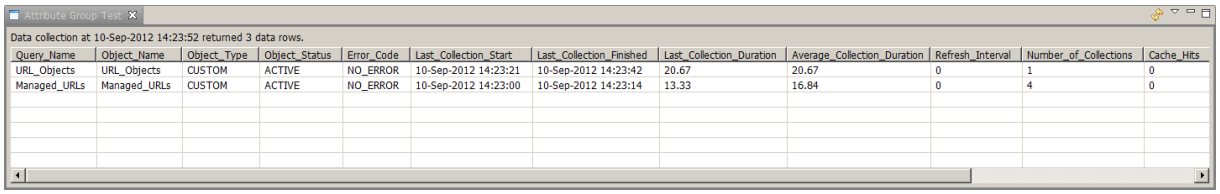


*Figura 69. Vista **Prueba de grupo de atributos** que muestra más información (Estatus de objeto de rendimiento) sobre recopilaciones de datos para los grupos de atributos **Managed_URLs** y **Managed_Nodes***

10. Cuando haya terminado de probar el agente, pulse el icono de detención del agente

Variables de entorno de prueba

Utilice estas variables de entorno para controlar el comportamiento del agente durante la prueba.

Las variables de entorno son valores dinámicos con nombre que determinan cómo se ejecuta el agente. En el caso de prueba de grupo de atributos, algunas variables de entorno del agente se establecen en valores especiales. Los valores especiales se utilizan para que el agente responda de forma que se adapte a la prueba de un grupo de atributos individual. Para la prueba de todo el agente no se utilizan valores especiales, en su lugar se utilizan los valores predeterminados. Los valores predeterminados implican que el agente se comporta como lo haría normalmente, que es más adecuado para la prueba de todo el agente.

Las variables de entorno que tienen valores especiales para la prueba de grupo de atributos se resumen en la tabla siguiente. Para obtener más información sobre todas las variables de entorno del agente, consulte “Lista de variables de entorno” en la página 1211. Para obtener más información sobre cómo establecer variables de entorno, consulte “Variables de entorno” en la página 1211.

Tabla 299. Variables de entorno			
Variable de entorno	**Valor predeterm. (prueba de todo el agente)**	**Valor de prueba de grupo de atributos**	**Razón para el cambio de valor para la prueba de grupo de atributos**
CDP_DP_INITIAL_COLLECTION_DELAY	varía	1	Este valor se aplica a un agente con una agrupación de hebras. Este valor es el tiempo, en segundos, que la agrupación de hebras espera antes de que la solicitud de recopilación de datos iniciales se envíe a un proveedor de datos. **Nota:** Si no se ha establecido CDP_DP_INITIAL_COLLECTION_DELAY , la agrupación de hebras espera por el tiempo que especifica CDP_DP_REFRESH_INTERVAL o CDP_ATTRIBUTE_GROUP_REFRESH_INTERVAL. Este tiempo de espera es el mismo tiempo que la agrupación de hebras espera entre las recopilaciones de datos, y el tiempo de espera para la primer recopilación de datos podría ser demasiado larga.
CDP_DP_CACHE_TTL	55	1	Cuando se establece en 1 es mucho más probable que una solicitud de recopilar datos recopile los datos inmediatamente. De lo contrario, puede devolver datos de la memoria caché con una antigüedad de hasta 60 segundos.

Instalación del agente en una infraestructura de supervisión para la realización de prueba s y el uso

Tras probar el agente en Agent Builder, puede instalar el agente en un entorno de IBM Tivoli Monitoring o IBM Cloud Application Performance Management existente para realizar más pruebas y para su uso.

La instalación y las pruebas del agente en una infraestructura de supervisión tiene las siguientes ventajas:

- Puede configurar y probar varias instancias de un agente que se ejecutan simultáneamente.
- Puede configurar y probar varias instancias de subnodos que se ejecutan simultáneamente.
- En un entorno Tivoli Monitoring, puede crear espacios de trabajo, situaciones, acciones y consultas en Tivoli Enterprise Portal.

Importante: Despliegue las versiones iniciales del agente en una versión de prueba de la infraestructura de supervisión. En Tivoli Monitoring, utilice un servidor de supervisión y un servidor de portal aparte. En Cloud APM, utilice una cuenta de nube o un despliegue de prueba aparte del servidor de supervisión local. Despliegue la versión final del agente en una infraestructura de producción.

Si despliega una versión del agente en la infraestructura de supervisión y a continuación cambia conjuntos de datos en el agente, es posible que se produzca un conflicto entre la versión nueva y la versión antigua del servidor. En tal caso será imposible utilizar cualquiera de las versiones del agente.

Instalación de un agente

Existen dos métodos para instalar los agentes que crea con Agent Builder.

1. Para probar el agente con una infraestructura de supervisión que se ejecuta en el mismo sistema que Agent Builder, puede instalar el agente en la instalación local de Tivoli Monitoring o Cloud APM.
2. Para probar o utilizar el agente con un sistema de Tivoli Monitoring o Cloud APM que no se está ejecutando en el mismo sistema que Agent Builder, puede generar un archivo comprimido (*paquete de agente*) que puede transferir a los otros sistemas y desplegar.

Nota:

1. Con Tivoli Monitoring, tras instalar un agente, podrá ver métricas de rendimiento en las tablas Tivoli Enterprise Portal. Para obtener soporte de situaciones o espacios de trabajo, consulte "Importación de archivos de soporte de aplicaciones" en la página 1444.
2. Con Tivoli Monitoring, tras instalar el agente, puede utilizar el Tivoli Enterprise Portal para verificar los datos del agente. Para obtener más información, consulte "Cambios en Tivoli Enterprise Portal" en la página 1438. Si después de ver los datos en Tivoli Enterprise Portal, desea modificar el agente, consulte "Utilización del editor del agente para modificar el agente" en la página 1208.
3. Para un agente que soporta Linux o UNIX, genere la imagen del instalador en un sistema Linux o UNIX porque un sistema Linux o UNIX crea los archivos los permisos apropiados.

Instalación de un agente localmente

Instalar el agente en un entorno de supervisión en el sistema local en el que se está ejecutando Agent Builder.

Acerca de esta tarea

Complete los pasos siguientes para instalar el agente en un entorno de supervisión en el sistema local:

1. Pulse el archivo `itm_toolkit_agent.xml` en el árbol de navegación del Explorador de proyectos de Agent Builder siguiendo uno de estos métodos:
   a. Pulse con el botón derecho el archivo `itm_toolkit_agent.xml` y seleccione **IBM** > **Generar agente**.
   b. Seleccione el archivo `itm_toolkit_agent.xml` y seleccione el icono  **Generar agente** en la barra de herramientas.
   c. Efectúe una doble pulsación en el archivo `itm_toolkit_agent.xml` y seleccione **Agent Editor** > **Generar agente**.
2. En la ventana **Asistente para generar agente**, en la sección **Instalar el agente localmente**, especifique el directorio de instalación de la infraestructura de supervisión. Agent Builder completa el valor que se encuentra en la variable de entorno `CANDLE_HOME`. Si la variable no se ha establecido, se visualiza el valor predeterminado para Windows, `C:\IBM\ITM`.

   Los recuadros de selección se habilitan como sigue:

   Instalar el agente
   Está habilitado si Agent Builder detecta un Tivoli Enterprise Monitoring Agent o un agente de IBM Cloud APM en la ubicación especificada. Un agente apropiado es uno que soporta el sistema operativo local y es la versión mínima correcta.

   Instalar el soporte de TEMS
   Está habilitado en un entorno de Tivoli Monitoring si Agent Builder detecta un Tivoli Enterprise Monitoring Server en la ubicación especificada.

   Instalar el soporte de TEPS
   Está habilitado en un entorno de Tivoli Monitoring si Agent Builder detecta un Tivoli Enterprise Portal Server en la ubicación especificada.
3. Seleccione los componentes que se van a instalar (agente, soporte del servidor de Tivoli Enterprise Monitoring, soporte del servidor de Tivoli Enterprise Portal).
4. En un entorno de Tivoli Monitoring, si Tivoli Enterprise Monitoring Server o Tivoli Enterprise Portal Server está instalado en el sistema local y está instalando los archivos de soporte para estos servidores, puede elegir si desea reiniciar los servidores.

En este caso, los recuadros de selección **Reiniciar TEMS sin credenciales** y **Reiniciar TEPS** están activos en la sección **Instalar el agente localmente** del asistente para generar agente. Puede desmarcar los recuadros de selección para instalar el soporte sin reciclar los servidores.

Cuando borra el recuadro de selección **Reiniciar TEMS sin credenciales**, se le solicita el ID de usuario y la contraseña del servidor de Tivoli Enterprise Monitoring. Especifique estos detalles y pulse **Inicio de sesión**. Si ejecuta Tivoli Monitoring con la seguridad desactivada, entre "sysadmin" para el ID de usuario, deje la contraseña en blanco y pulse **Iniciar sesión**.

Como alternativa, para continuar si entrar credenciales, pulse **Iniciar sesión** si especificar un ID de usuario y una contraseña y pulse **Cancelar**. Si sigue estos pasos, Tivoli Enterprise Monitoring Server se reinicia.

Importante: Para instalar archivos de soporte sin reiniciar Tivoli Enterprise Monitoring Server, asegúrese de que Tivoli Enterprise Monitoring Server está en ejecución.

5. Seleccione los componentes del agente para generar. Puede seleccionar **Agente base**, **Cognos Reporting**, o ambos.
6. En un entorno de IBM Cloud APM, puede proporcionar firma de seguridad para los agentes de autodescripción. Pulse **Editar todas las preferencias de firma JAR**. Puede añadir una indicación de fecha y hora a los archivos JAR firmados y especificar la autoridad de indicación de fecha y hora. Especifique detalles sobre el archivo de almacén de claves Java.

   Nota: Debe crear el archivo de almacén de claves Java utilizando herramientas Java. Por ejemplo, para generar una clave privada y un certificado con una clave pública correspondiente en un archivo de almacén de claves Java, puede ejecutar este mandato:

   - `vía_instalación_ab/jre/bin/keytool -genkeypair -keystore vía_archivo_almacén_claves -storepass contraseña_almacén_claves -alias alias_almacén_claves -dname "CN=nombre_común, OU=unidad_organizativa, L=ciudad_o_localidad, ST=estado_o_provincia, C=país" -keypass contraseña_clave`

   Donde:

   - *vía_instalación_ab* es la ubicación donde se instala Agent Builder
   - *vía_archivo_almacén_claves* es la vía de acceso en la que hay un almacén de claves JKS existente o en la que se crea uno
   - *contraseña_almacén_claves* es la contraseña necesaria para acceder a cualquier elemento de este almacén de claves
   - *alias_almacén_claves* es un nombre que identifica esta clave dentro del almacén de claves (adopta como valor predeterminado `"mykey"`)
   - *contraseña_clave* la contraseña necesaria para acceder a esta clave particular (adopta como valor predeterminado `key_store_password`)

   El certificado se debe incluir en el almacén de claves para el servidor.
7. Cuando complete los detalles de **Firmado de JAR**, pulse **Aceptar**.
8. Pulse **Finalizar**.
9. Configure e inicie el agente. Para obtener más información, consulte “Configurar e iniciar el agente en un entorno IBM Tivoli Monitoring” en la página 1431 o “Configuración del agente” en la página 1433 y “Inicio y detención del agente” en la página 1434 en un entorno de IBM Cloud APM.

   Para Tivoli Monitoring v6.2 FP1 o posterior, puede instalar el soporte del servidor de Tivoli Enterprise Monitoring y del servidor de Tivoli Enterprise Portal sin reiniciar los servidores. En este caso, los recuadros de selección **Reiniciar TEMS sin credenciales** y **Reiniciar TEPS** están activos en la sección **Instalar el agente localmente** del asistente para generar agente. Puede desmarcar los recuadros de selección para instalar el soporte sin reciclar los servidores. Cuando borra el recuadro de selección **Reiniciar TEMS sin credenciales**, se le solicita el ID de usuario y la contraseña del servidor de Tivoli Enterprise Monitoring. Especifique el ID de usuario y la contraseña del servidor de Tivoli Enterprise Monitoring y pulse **Iniciar sesión**. Si ejecuta Tivoli Monitoring con la seguridad desactivada, entre

"sysadmin" para el ID de usuario, deje la contraseña en blanco y pulse **Iniciar sesión**. También puede continuar sin especificar credenciales (pulse **Iniciar sesión** sin especificar un ID de usuario y contraseña o pulse **Cancelar**; si hace esto, el servidor de Tivoli Enterprise Monitoring se reciclará).

Nota: El servidor de Tivoli Enterprise Monitoring debe estar en ejecución para instalar los archivos de soporte, sin reciclar el servidor de Tivoli Enterprise Monitoring.

Creación del paquete de agente
Puede utilizar Agent Builder para crear un paquete de instalación de agente comprimido.

Acerca de esta tarea

Un paquete de agente contiene todos los archivos necesarios para ejecutar el agente, así como los scripts de instalación y configuración. El paquete también incluye archivos de soporte para el entorno de supervisión.

Puede utilizar un paquete de agente para instalar el agente en los entornos de IBM Tivoli Monitoring e IBM Cloud Application Performance Management.

Procedimiento

1. Pulse el archivo `itm_toolkit_agent.xml` en el árbol de navegación **Explorador de proyectos** de Agent Builder siguiendo uno de estos métodos:
   - Pulse con el botón derecho el archivo `itm_toolkit_agent.xml` y seleccione **IBM** > **Generar agente**.
   - Seleccione el archivo `itm_toolkit_agent.xml` y seleccione el icono  **Generar agente** en la barra de herramientas.
   - Efectúe una doble pulsación en el archivo `itm_toolkit_agent.xml` y seleccione **Agent Editor** > **Generar agente**.
2. Escriba el nombre del directorio donde desea poner la salida (un paquete comprimido o archivos ampliados) en la sección **Generar imagen de agente**.
3. Marque el recuadro de selección **Mantener archivos intermedios** para mantener los archivos ampliados generados separados del archivo zip o tar.
4. Seleccione **Crear un archivo ZIP** para crear un archivo comprimido en el directorio especificado. El archivo zip comprimido se llama `smai-`*`nombre_agente-versión`*`.zip` para los sistemas Windows, de forma predeterminada.
5. Marque el recuadro de selección **Crear un archivo TAR** para crear un archivo tar en el directorio especificado. El archivo tar comprimido se llama `smai-`*`nombre_agente-versión`*`.tgz` para los sistemas UNIX y Linux, de forma predeterminada.
6. Seleccione los componentes del agente para generar. Puede seleccionar **Agente base**, **Cognos Reporting**, o ambos.

   Importante: Para el entorno IBM Cloud Application Performance Management, seleccione los informes **Cognos Reporting**, porque los informes no están soportados actualmente e incluir los informes aumenta el tamaño del paquete.
7. De forma opcional, puede proporcionar firma de seguridad para archivos de aplicación de agente. Si quiere proporcionar firmado de seguridad, seleccione **Firmar JAR de soporte de autodescripción**. Pulse **Editar todas las preferencias de firma JAR**. Puede añadir una indicación de fecha y hora a los archivos jar firmados y especificar la autoridad de indicación de fecha y hora. Especifique detalles sobre el archivo de almacén de claves Java.

   Importante: Puede crear el archivo de almacén de claves Java utilizando herramientas Java. Por ejemplo, para generar una clave privada y un certificado con una clave pública correspondiente en un archivo de almacén de claves Java, puede ejecutar este mandato:

   - *`vía_instalación_ab`*`/jre/bin/keytool -genkeypair -keystore` *`vía_archivo_almacén_claves`* `-storepass` *`contraseña_almacén_claves`* `-alias` *`alias_almacén_claves`* `-dname "CN=`*`nombre_común`*`, OU=`*`unidad_organizativa`*`,`

L=*ciudad_o_localidad*, ST=*estado_o_provincia*, C=*país*" -keypass *contraseña_clave*

Donde:

- *vía_instalación_ab* es la ubicación donde se instala Agent Builder
- *vía_archivo_almacén_claves* es la vía donde reside un almacén de claves JKS existente, o donde se creará uno
- *contraseña_almacén_claves* es la contraseña necesaria para acceder a cualquier elemento de este almacén de claves
- *alias_almacén_claves* es un nombre que identifica esta clave dentro del almacén de claves (adopta como valor predeterminado "mykey")
- *contraseña_clave* es la contraseña necesaria para acceder a esta clave particular (adopta como valor predeterminado key_store_password)

Incluya este certificado en el almacén de claves del servidor.

8. Pulse **Finalizar**.

Instalación del paquete en un entorno IBM Tivoli Monitoring

Para probar o utilizar el agente en el entorno de IBM Tivoli Monitoring, utilice el paquete generado para instalar el agente en sistemas supervisados, sistemas de servidores de supervisión de hub y sistema de Portal Server.

Antes de empezar

Antes de instalar el agente en un sistema supervisado, asegúrese de que el agente del sistema operativo de Tivoli Monitoring está presente y en funcionamiento. Para obtener información sobre la instalación de agentes de Tivoli Monitoring, consulte Instalación de agentes de supervisión en Tivoli Monitoring Knowledge Center.

Importante: Para visualizar información de agente en Tivoli Enterprise Portal, debe instalar los siguientes componentes:

- El agente en todos los sistemas supervisados
- Los archivos de soporte de Tivoli Enterprise Monitoring Server en el hub de Tivoli Enterprise Monitoring Servers
- Los archivos de soporte de Tivoli Enterprise Portal Server en Tivoli Enterprise Portal Server
- Los archivos de soporte de Tivoli Enterprise Portal en Tivoli Enterprise Portal Server y, si es aplicable, todos los clientes de escritorio de Tivoli Enterprise Portal.

Procedimiento

1. Copie el archivo comprimido, que se denomina *código_producto*.zip para sistemas Windows o *código_producto*.tgz para sistemas UNIX y Linux de forma predeterminada, en el sistema donde desea instalar el agente.
2. Extraiga el archivo en una ubicación temporal.

   Nota: Linux AIX Para los sistemas UNIX y Linux, esta ubicación temporal no puede ser /tmp/*código_producto*, donde el código de producto está en minúsculas.

   Puede instalar el agente de forma remota utilizando el archivo comprimido.

   - Linux En un sistema Linux, utilice el siguiente mandato para extraer el archivo .tgz:

     ```
     tar -xvzf nombre_archivo
     ```

   - UNIX En un sistema AIX, utilice el siguiente mandato para extraer el archivo .tgz:

     ```
     gunzip nombre_archivo
     tar -xvf nombre_archivo
     ```

3. Ejecute el script de instalación adecuado.
   - Para instalar el agente, Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server y Tivoli Enterprise Portal se soportan todos a la vez:

     ```
     InstallIra.bat/.sh ubicación_instalación_itm [[-h nombre_host_TEMS_concentrador] -u
     nombre_usuario_TEMS_concentrador -p contraseña_TEMS_concentrador]
     ```

   - Para instalar el agente sin instalar archivos de soporte:

     ```
     installIraAgent.bat/.sh ubicación_instalación_itm
     ```

   - Para instalar el soporte del servidor de Tivoli Enterprise Monitoring:

     ```
     installIraAgentTEMS.bat/.sh ubicación_instalación_itm [[-h nombre_host_TEMS_concentrador]
     -u
     nombre_usuario_TEMS_concentrador -p contraseña_TEMS_concentrador]
     ```

   - Para instalar el soporte de servidores de Tivoli Enterprise Portal y Tivoli Enterprise:

     ```
     installIraAgentTEPS.bat/.sh ubicación_instalación_itm
     ```

   La ubicación de instalación, *ubicación_instalación_itm* debe ser el primer argumento y es obligatorio en todos los scripts: `installIra.bat/.sh`, `installIraAgent.bat/.sh`, `installIraAgentTEMS.bat/.sh` y `installIraAgentTEPS.bat/.sh`. Esta es la ubicación donde los componentes de Tivoli Monitoring están instalados en este sistema.

   Otros argumentos son opcionales.

   Si se instalan archivos de soporte de Monitoring Server y no se proporciona un ID de usuario, Tivoli Enterprise Monitoring Server se reinicia.
4. Configure e inicie el agente: consulte "Configurar e iniciar el agente en un entorno IBM Tivoli Monitoring" en la página 1431.

Qué hacer a continuación

Si ha cambiado el diseño del agente de forma que los elementos del navegador se desplacen o eliminen, reinicie Tivoli Enterprise Portal Server y Tivoli Enterprise Portal. El reinicio asegura que los cambios se reconozcan correctamente.

Configurar e iniciar el agente en un entorno IBM Tivoli Monitoring

Después de instalar un agente en un sistema supervisado en IBM Tivoli Monitoring, configure e inicie el agente.

Procedimiento

1. Abra el **Manage Tivoli Monitoring Service**.

   Se visualiza la nueva entrada **Monitoring Agent for *nombre_agente***.
2. Pulse con el botón derecho del ratón en la entrada y seleccione **Configurar utilizando los valores predeterminados**. Si se le solicita, pulse **Aceptar** para aceptar los valores predeterminados.

   Importante:

   a. En los sistemas UNIX, la opción que se debe seleccionar es **Configurar**.

   b. Para agentes de varias instancias, al realizar la configuración se le solicita un nombre de instancia.

   Consejo: Si el agente utiliza un origen de datos JMX para conectar con un WebSphere Application Server remoto, asegúrese de que WebSphere Application Server también esté instalado en el host que está ejecutando el agente y establezca el valor de `Java Home` en el entorno de tiempo de ejecución Java que utiliza el WebSphere Application Server local.

Consejo: Para un origen de datos de API de Java, JDBC, JMX, HTTP o SOAP, puede utilizar los valores de **Java** > **Argumentos de JVM** para controlar el registro de rastreo de agente. Establezca el siguiente valor en esta configuración:

```
-DJAVA_TRACE_MAX_FILES=archivos -DJAVA_TRACE_MAX_FILE_SIZE=tamaño
```

onde *archivos* es el número máximo de archivos de registro de rastreo que se mantienen (el valor predeterminado es 4) y *tamaño* es el máximo tamaño de archivo de registro en kilobytes (el valor predeterminado es 5000). Por ejemplo, puede establecer el siguiente valor:

```
-DJAVA_TRACE_MAX_FILES=7 -DJAVA_TRACE_MAX_FILE_SIZE=100
```

En este caso, el agente graba 100 kilobytes en el primer archivo de registro y, a continuación, conmuta al segundo archivo de registro, y así sucesivamente. Después de grabar siete archivos de registro de 100 kilobytes cada uno, se graba encima del primer archivo de registro.

Si ha añadido elementos de configuración de tiempo de ejecución al agente, o si ha seleccionado un origen de datos, se visualizarán paneles de configuración. Utilice estos paneles para recopilar la información necesaria para el agente.

3. Pulse con el botón derecho del ratón en la entrada de agente y seleccione **Iniciar**
4. Abra Tivoli Enterprise Portal y vaya al nuevo agente.

Instalación y utilización de un agente en un entorno IBM Cloud Application Performance Management

Para probar o utilizar el agente en el entorno de IBM Cloud Application Performance Management, utilice el paquete generado para instalar el agente en todos los sistemas supervisados. En algunos casos será necesario configurar el agente para poder iniciarlo. Puede iniciar y detener el agente según sea necesario.

Instalación del agente

Utilice el paquete de instalación preparado por Agent Builder para instalar el agente en todos los sistemas supervisados.

Antes de empezar

Asegúrese de que en el sistema operativo ya está presente un agente para IBM Cloud Application Performance Management, normalmente el agente del sistema operativo, y que está en funcionamiento.

Windows En sistemas Windows, utilice un shell de línea de mandatos de administrador para instalar y configurar los agentes. Para iniciar un shell de administrador, seleccione **Símbolo del sistema** en el menú Programas de Windows, pulse con el botón derecho del ratón y pulse **Ejecutar como administrador**.

Procedimiento

1. Extraiga el paquete en un directorio temporal y vaya a ese directorio.
2. Instale el agente utilizando el mandato siguiente, en función del sistema operativo:
   - Windows En sistemas Windows, `installIraAgent.bat` *ubicación_agente_instalación*
   - Linux AIX En sistemas Linux y UNIX, `./installIraAgent.sh` *ubicación_instalación_agente*

   Donde *ubicación_instalación_agente* es la ubicación de la instalación del agente existente. La ubicación predeterminada es:

   - Windows En sistemas Windows,`C:\IBM\APM`
   - Linux En sistemas Linux, `/opt/ibm/apm/agent`
   - AIX En sistemas AIX, `/opt/ibm/apm/agent`

   Importante: Si ha añadido alguna propiedad de configuración personalizada en la ventana de **Configuración de tiempo de ejecución** del editor del agente, si el agente soporta varias instancias, o si el agente utiliza cualquier origen de datos predefinido que necesita configuración (por ejemplo, un

ID de usuario y una contraseña), debe configurar el agente para poder iniciarlo. Si un agente no requiere configuración, se inicia automáticamente tras la instalación.

Configuración del agente
Si ha añadido alguna propiedad de configuración personalizada en la ventana de configuración del tiempo de ejecución del editor del agente, si el agente soporta varias instancias, o si el agente utiliza cualquier origen de datos predefinido que necesita configuración (por ejemplo, un ID de usuario y una contraseña), debe configurar el agente para poder iniciarlo.

Antes de empezar

Windows En sistemas Windows, utilice un shell de línea de mandatos de administrador para instalar y configurar los agentes. Para iniciar un shell de administrador, seleccione **Símbolo del sistema** en el menú Programas de Windows, pulse con el botón derecho del ratón y pulse **Ejecutar como administrador**.

Acerca de esta tarea
En el proceso de configuración, puede:

- Establecer el nombre de instancia para crear o cambiar una instancia, si el agente da soporte a varias instancias.
- Establecer las propiedades de configuración que estén disponibles para el agente.
- Crear y configurar subnodos, si el agente da soporte a subnodos.

Windows En sistemas Windows, para establecer propiedades de configuración o crear subnodos, debe utilizar el procedimiento de configuración silenciosa. Encontrará un archivo de respuestas de configuración silenciosa de ejemplo en el directorio *dir_instalación*\samples, denominado *nombre_agente*_silent_config.txt. Cree una copia de este archivo y establezca las variables de configuración según se requiera.

Linux AIX En sistemas Linux y UNIX, puede utilizar opcionalmente el procedimiento de configuración silenciosa. Como alternativa, puede utilizar el procedimiento interactivo. Si inicia el mandato de configuración sin un nombre de archivo de respuestas, el programa de utilidad de configuración le solicitará los valores de configuración.

Procedimiento

1. Vaya al directorio *dir_instalación*/bin.
2. Ejecute el siguiente mandato para configurar el agente:
   - Si el agente no soporta varias instancias:
     - Windows En sistemas Windows, *nombre*-agent.bat config [*archivo_respuestas*]
     - Linux AIX En sistemas Linux y UNIX, ./*nombre*-agent.sh config [*archivo_respuestas*]
   - Si el agente soporta varias instancias:
     - Windows En sistemas Windows, *nombre*-agent.bat config *nombre_instancia* [*archivo_respuestas*]
     - Linux AIX En sistemas Linux y UNIX, ./*nombre*-agent.sh config *nombre_instancia* [*archivo_respuestas*]

   Donde:

   - *nombre_instancia* es el nombre de la instancia. Si no existe una instancia con ese nombre, la instancia se creará. Si ya existe la instancia, se reconfigurará. Para utilizar el agente debe crear al menos una instancia.
   - *archivo_respuestas* es el nombre del archivo de respuestas de configuración silenciosa.

Consejo: Si el agente utiliza un origen de datos JMX para conectar con un WebSphere Application Server remoto, asegúrese de que WebSphere Application Server también esté instalado en el host que está ejecutando el agente y establezca el valor de `Java Home` en el entorno de tiempo de ejecución Java que utiliza el WebSphere Application Server local.

Consejo: Para un origen de datos de API de Java, JDBC, JMX, HTTP o SOAP, puede utilizar los valores de **Java** > **Argumentos de JVM** para controlar el registro de rastreo de agente. Establezca el siguiente valor en esta configuración:

```
-DJAVA_TRACE_MAX_FILES=archivos -DJAVA_TRACE_MAX_FILE_SIZE=tamaño
```

onde *archivos* es el número máximo de archivos de registro de rastreo que se mantienen (el valor predeterminado es 4) y *tamaño* es el máximo tamaño de archivo de registro en kilobytes (el valor predeterminado es 5000). Por ejemplo, puede establecer el siguiente valor:

```
-DJAVA_TRACE_MAX_FILES=7 -DJAVA_TRACE_MAX_FILE_SIZE=100
```

En este caso, el agente graba 100 kilobytes en el primer archivo de registro y, a continuación, conmuta al segundo archivo de registro, y así sucesivamente. Después de grabar siete archivos de registro de 100 kilobytes cada uno, se graba encima del primer archivo de registro.

Inicio y detención del agente

Para supervisar un sistema, asegúrese de que el agente se ha iniciado en el sistema. Puede iniciar y detener el agente en cualquier momento. Si el agente soporta varias instancias, puede iniciar y detener cada una de las instancias de forma independiente.

Procedimiento

1. Vaya al directorio *dir_instalación*/bin.
2. Ejecute el mandato siguiente para iniciar el agente:
   - Si el agente no soporta varias instancias:
     - Windows En sistemas Windows, *nombre*-agent.bat start
     - Linux AIX En sistemas Linux y UNIX, ./*nombre*-agent.sh start
   - Si el agente soporta varias instancias:
     - Windows En sistemas Windows, *nombre*-agent.bat start *nombre_instancia*
     - Linux AIX En sistemas Linux y UNIX, ./*nombre*-agent.sh start *nombre_instancia*
3. Ejecute el mandato siguiente para detener el agente:
   - Si el agente no soporta varias instancias:
     - Windows En sistemas Windows, *nombre*-agent.bat stop
     - Linux AIX En sistemas Linux y UNIX, ./*nombre*-agent.sh stop
   - Si el agente soporta varias instancias:
     - Windows En sistemas Windows, *nombre*-agent.bat stop *nombre_instancia*
     - Linux AIX En sistemas Linux y UNIX, ./*nombre*-agent.sh stop *nombre_instancia*

Resultados tras generación e instalación del agente

La instalación de un agente de Agent Builder crea y cambia determinados archivos en el sistema. En un entorno de IBM Tivoli Monitoring, también puede ver los cambios en Tivoli Enterprise Portal.

Nuevos archivos en el sistema

Tras generar e instalar el agente que ha creado con Agent Builder, puede ver los archivos nuevos siguientes en el sistema del agente:

Nota: *xx* indica el código de producto de dos caracteres.

Windows

Sistemas Windows:

TMAITM6\k*xx*agent.exe
Binario del agente

TMAITM6\K*xx*ENV
Valores de variables de entorno

TMAITM6\K*xx*.ref
Configuración del proveedor de agente

TMAITM6\SQLLIB\k*xx*.his
Descripción SQL de la información de atributo del agente

TMAITM6\SQLLIB\k*xx*.atr
Información de atributo del agente

TMAITM6*xx*_dd_*versión*.xmll
Descripción del producto

TMAITM6*xx*_dd.properties
Nombre del producto

TMAITM6\kxxcma.ini
Archivo de definición de servicio del agente

TMAITM6*los archivos*
Los archivos complementarios incluidos de la API Java o los orígenes de datos de socket con un tipo de archivo de *executable* o *library*. Los scripts incluidos desde el Script o el Mandato devuelven orígenes de datos de código.

Linux AIX

Sistemas UNIX/Linux:

registry/*xx*arquitectura*.ver
Versiones internas y archivo de requisitos previos

***architecture*/*xx*/bin/*xx*_dd_*versión*.xml**
Descripción del producto

***arquitectura*/*xx*/bin/k*xx*agente**
Binario del agente

***arquitectura*/*xx*/bin/*xx*_dd.properties**
Nombre del producto

***arquitectura*/*xx*/work/k*xx*.ref**
Configuración del proveedor de agente

***arquitectura*/*xx*/tables/ATTRLIB/k*xx*.atr**
Información de atributo del agente

***arquitectura*/*xx*/hist/k*xx*.his**
Descripción SQL de la información de atributo del agente

arquitectura*/*xx*/bin/*los archivos
Archivos suplementarios incluidos de los orígenes de datos de API o Socket de Java con un tipo de archivo *ejecutable*. Los scripts incluidos desde el Script o el Mandato devuelven orígenes de datos de código.

arquitectura*/*xx*/lib/*sus archivos
Archivos suplementarios incluidos los orígenes de datos de socket o de API de Java con un tipo de archivo Biblioteca.

config/.*xx*.rc
Archivo de configuración interna

config/*xx*.environment
Valores de entorno

config/*xx*_dd_*versión*.xml
Descripción del producto

config/*xx*_dd.properties
Nombre del producto

config/.ConfigData/k*xx*env
Valores de variables de entorno

Nota: Ejecute el mandato siguiente para averiguar la arquitectura del sistema:

```
cinfo -p xx
```

donde *xx* es un código de producto de dos caracteres.

Por ejemplo, para un sistema Solaris 8 de 64 bits que ejecuta un agente con el código de producto 19, la salida es la siguiente:

```
# /opt/ibm/apm/agent/bin/cinfo -p 19

*********** Fri Aug 17 11:23:58 EDT 2007 ******************
User : root Group: other
Host name : guadalajara  Installer Lvl:06.20.00.00
CandleHome: /opt/IBM/ITM
***********************************************************
Platform codes:
sol286 : Current machine
sol286 : Producto (19)
tmaitm6/sol286 : CT Framework (ax)
```

La línea en negrita es la relevante. La cadena antes de los dos puntos, sol286, indica la arquitectura en uso para este agente. Esta cadena es diferente para las distintas combinaciones de sistema operativo y tipo de hardware del sistema. El agente debe haberse instalado previamente para que esta característica funcione.

Los archivos siguientes son para orígenes de datos con base Java. Estos archivos solo se crean si el agente contiene orígenes de datos JMX, JDBC, HTTP o SOAP:

- cpci.jar
- jlog.jar
- common/jatlib-1.0.jar

Los archivos siguientes son para el soporte de tiempo de ejecución JMX. Estos archivos se crean solo si el agente contiene orígenes de datos JMX:

- common/jmx-1.0.jar
- common/connectors/jboss/connJboss-1.0.jar
- common/connectors/jsr160/connJSR160-1.0.jar
- common/connectors/was/connWas-1.0.jar
- common/connectors/weblogic/connWeblogic-1.0.jar

El siguiente archivo es para soporte de tiempo de ejecución JDBC. Estos archivos solo se crean si el agente contiene orígenes de datos JDBC:

- common/jdbc-1.0.jar

El siguiente archivo es para soporte de tiempo de ejecución HTTP o SOAP. Estos archivos solo se crean si el agente contiene orígenes de datos HTTP o SOAP:

- http-1.0.jar

Los archivos siguientes son para el soporte de tiempo de ejecución de Java API. Estos archivos se crean solo si el agente contiene un origen de datos de Java API:

- `cpci.jar`
- `custom/`*`el archivo JAR`* El nombre de este archivo JAR se especifica en los **Valores globales** de un origen de datos de la API de Java.
- `custom/`*`archivo JAR`* Archivos suplementarios con un tipo de archivo de recurso Java.

Los mismos archivos existen en sistemas Windows, UNIX y Linux para orígenes de datos con base Java, pero están en directorios diferentes:

- Windows Vía de acceso en Windows: `TMAITM6\kxx\jars`
- Linux AIX Vía de acceso en UNIX/Linux: *`arquitectura`*`/`*`xx`*`/jars`

Los archivos siguientes son para el soporte de tiempo de ejecución de la supervisión de archivos de registro. Estos archivos solo se crean si el agente contiene orígenes de datos del archivo de registro:

- Windows En sistemas Windows: TMAITM6\kxxudp.dll
- Linux En sistemas Solaris/Linux: *architecture*/*xx*/lib/libkxxudp.so
- En sistemas HP-UX: *architecture*/*xx*/lib/libkxxudp.sl
- UNIX En sistemas AIX: *architecture*/*xx*/lib/libkxxudp.a

Los archivos siguientes son para el soporte de tiempo de ejecución de supervisión del script SSH. Estos archivos solo se crean si el agente contiene un origen de datos de script que está habilitado para la colección SSH:

- Windows En sistemas Windows: `TMAITM6\kxxssh.dll`
- Linux En sistemas Solaris/Linux: *`arquitectura`*`/`*`xx`*`/lib/libkxxssh.so`
- En sistemas HP-UX: *`arquitectura`*`/`*`xx`*`/lib/libkxxssh.sl`
- UNIX En sistemas AIX: *`arquitectura`*`/`*`xx`*`/lib/libkxxssh.a`

Cambios en la ventana Manage Tivoli Enterprise Monitoring Services

Después de instalar un agente en un entorno de IBM Tivoli Monitoring, puede ver una entrada para el agente en la ventana **Manage Tivoli Enterprise Monitoring Services**. El nombre de la entrada es **Monitoring Agent for *nombre_agente***.

Importante: Manage Tivoli Enterprise Monitoring Services no está soportado en el entorno IBM Cloud Application Performance Management.

Windows En sistemas Windows, esta entrada contiene una columna **Tarea/Subsistema** que identifica si el agente soporta varias instancias:

- Un agente de instancia única muestra una nueva aplicación en la ventana **Manage Tivoli Enterprise Monitoring Services**. EL nombre de la aplicación es **Monitoring Agent for *nombre_agente***. Se crea un servicio para el agente (Figura 70 en la página 1438). La columna **Task/Subsystem** contiene el valor **Primario**.
- Un agente de varias instancias muestra una nueva plantilla de aplicación en la ventana **Manage Tivoli Enterprise Monitoring Services**. El nombre de la plantilla es **Monitoring Agent for *nombre_agente***. No se crea un servicio para el agente hasta que se crea una instancia del agente desde esta plantilla. La columna **Tarea/Subsistema** contiene el valor **Plantilla** para indicar que esta entrada es una plantilla que se utiliza para crear instancias del agente.

Linux AIX En sistemas Linux y UNIX, la entrada para el agente es la misma si el agente soporta varias instancias o no.

Nota: Las pantallas siguientes para un sistema Windows. Los sistemas UNIX y Linux tienen pantallas similares.

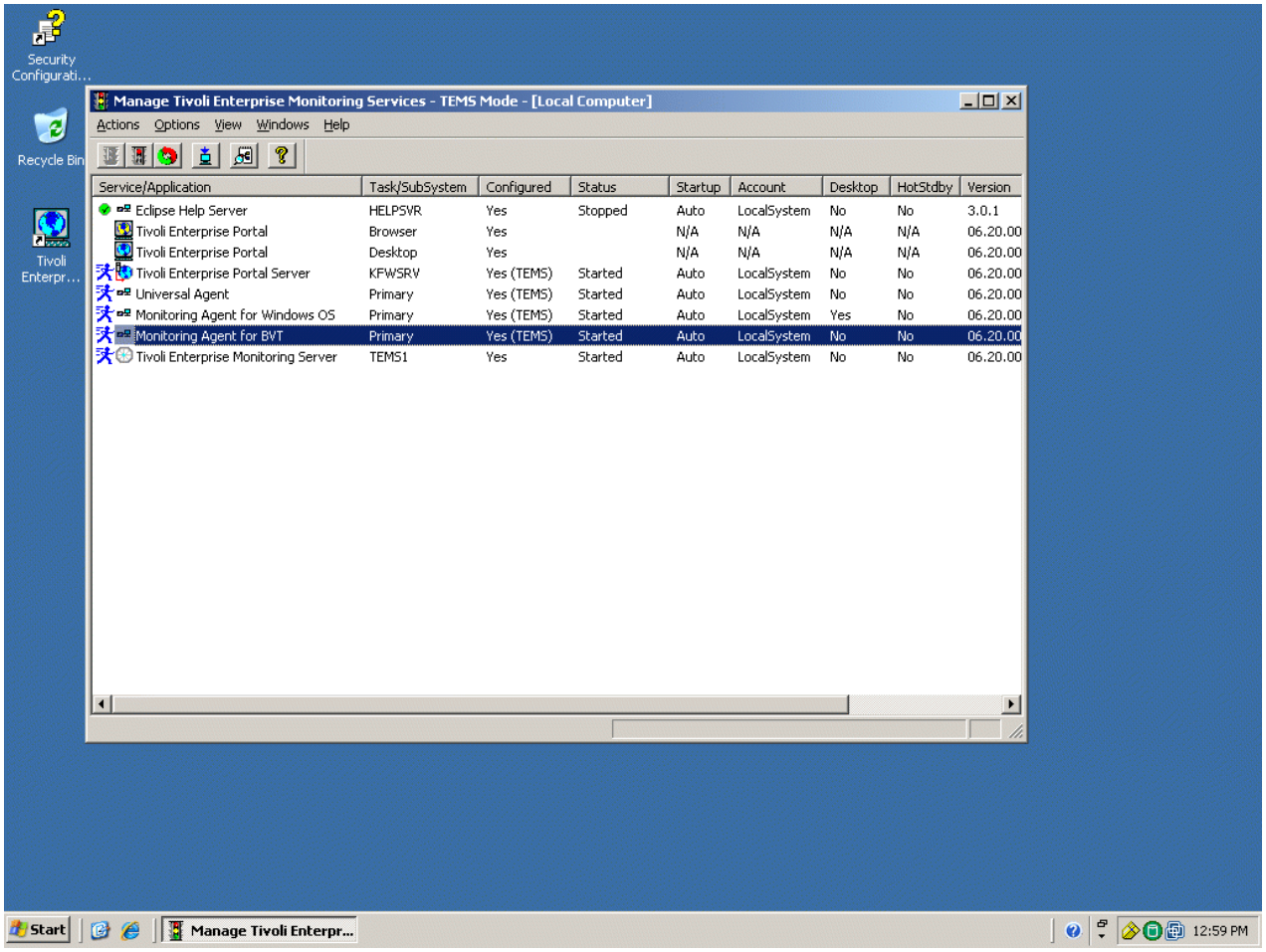


Figura 70. Ventana Manage Tivoli Enterprise Monitoring Services

Cambios en Tivoli Enterprise Portal

En un entorno de IBM Tivoli Monitoring, después de instalar e iniciar el agente, pulse el icono **Renovar** verde en Tivoli Enterprise Portal. A continuación podrá ver el nuevo agente. Puede ver los siguientes cambios en el portal:

- Un nuevo subnodo para el agente en la vista física de Tivoli Enterprise Portal.
- Nodos para cada grupo de Navigator y origen de datos de nivel superior que haya definido utilizando Agent Builder (Figura 71 en la página 1439).

  Nota: Para cada elemento de Navigator, debe definir una consulta predeterminada.

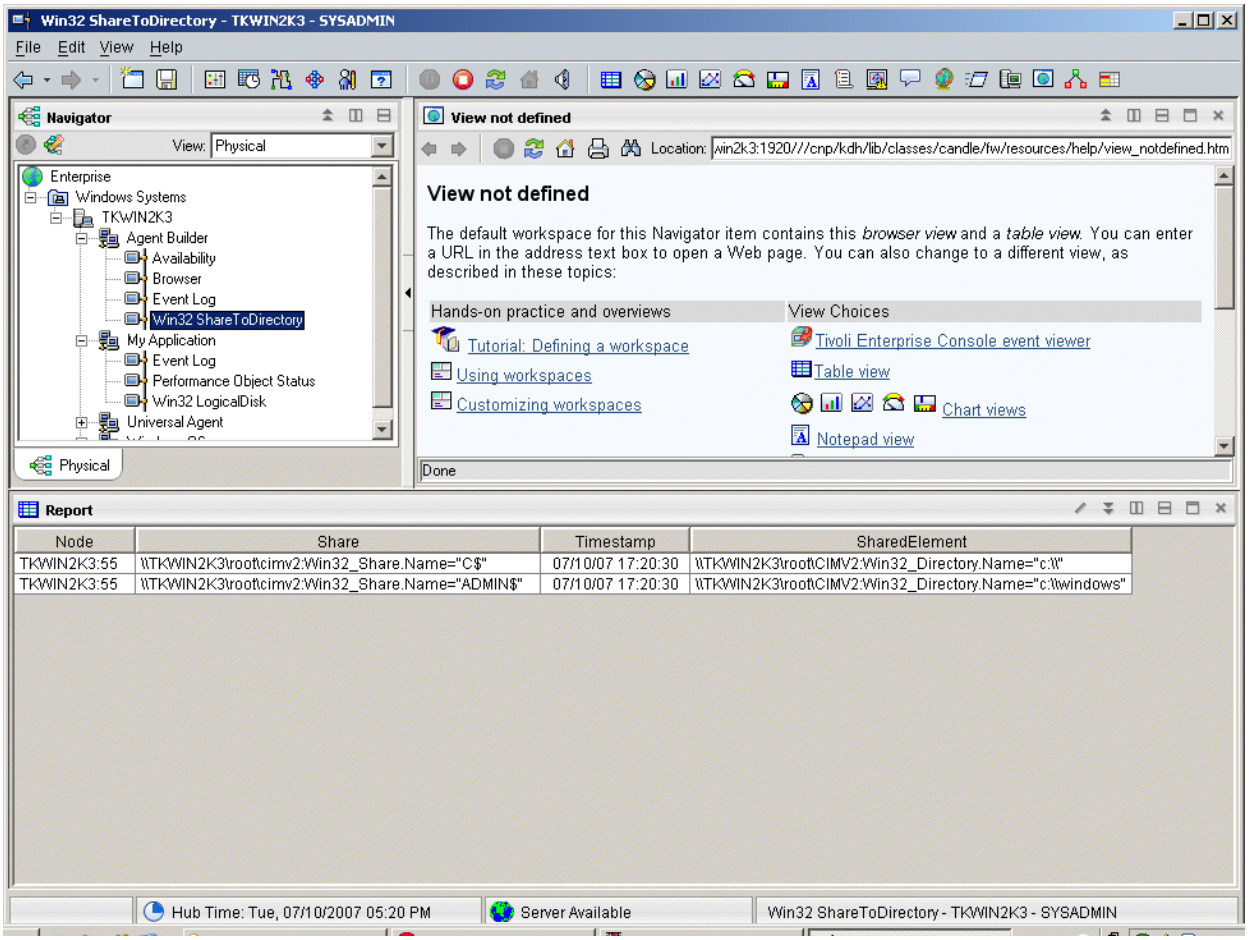


Figura 71. Nodos para grupos de atributos en el nuevo agente.

- Si el agente contiene subnodos, habrá un nodo expandible para cada subnodo definido en el agente. Los nodos siguientes se muestran bajo el nodo expandible:
  - Estado de objeto de rendimiento xxx, donde xxx es un tipo de subnodo de tres letras
  - Nodos para todos los grupos de Navigator y los orígenes de datos que se hayan definido en el subnodo
  - Nodo de registro de suceso de xxx si existen registros de suceso
  - Nodo de supervisores JMX de xxx si existe JMX y se han incluido supervisores de JMX
- El siguiente nodo automático:
  - Un nodo de disponibilidad si el agente contiene un origen de datos de disponibilidad (Figura 72 en la página 1440)

    Nota: Dicho nodo se comporta de forma distinta en función del contenido del agente. Si el agente supervisa solo la disponibilidad, el nodo de disponibilidad representa el origen de datos de disponibilidad. Si el agente supervisa la disponibilidad y el rendimiento, el nodo de disponibilidad se convierte en el elemento de navegador que representa los orígenes de datos del estado del objeto de rendimiento y disponibilidad.

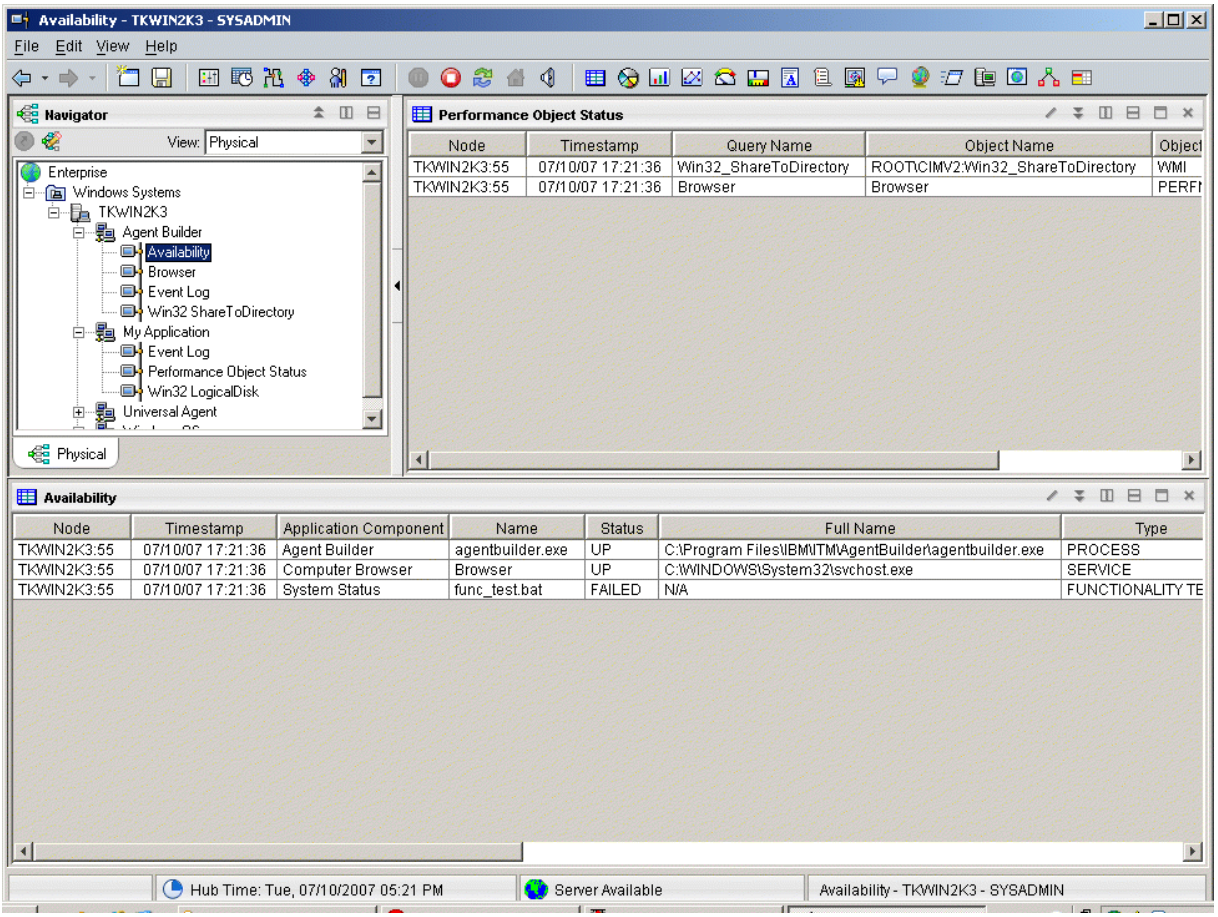


Figura 72. Nodo de disponibilidad

– Estado de objeto de rendimiento, si el agente incluye orígenes de datos de la supervisión de rendimiento (no la disponibilidad) (Figura 73 en la página 1441)

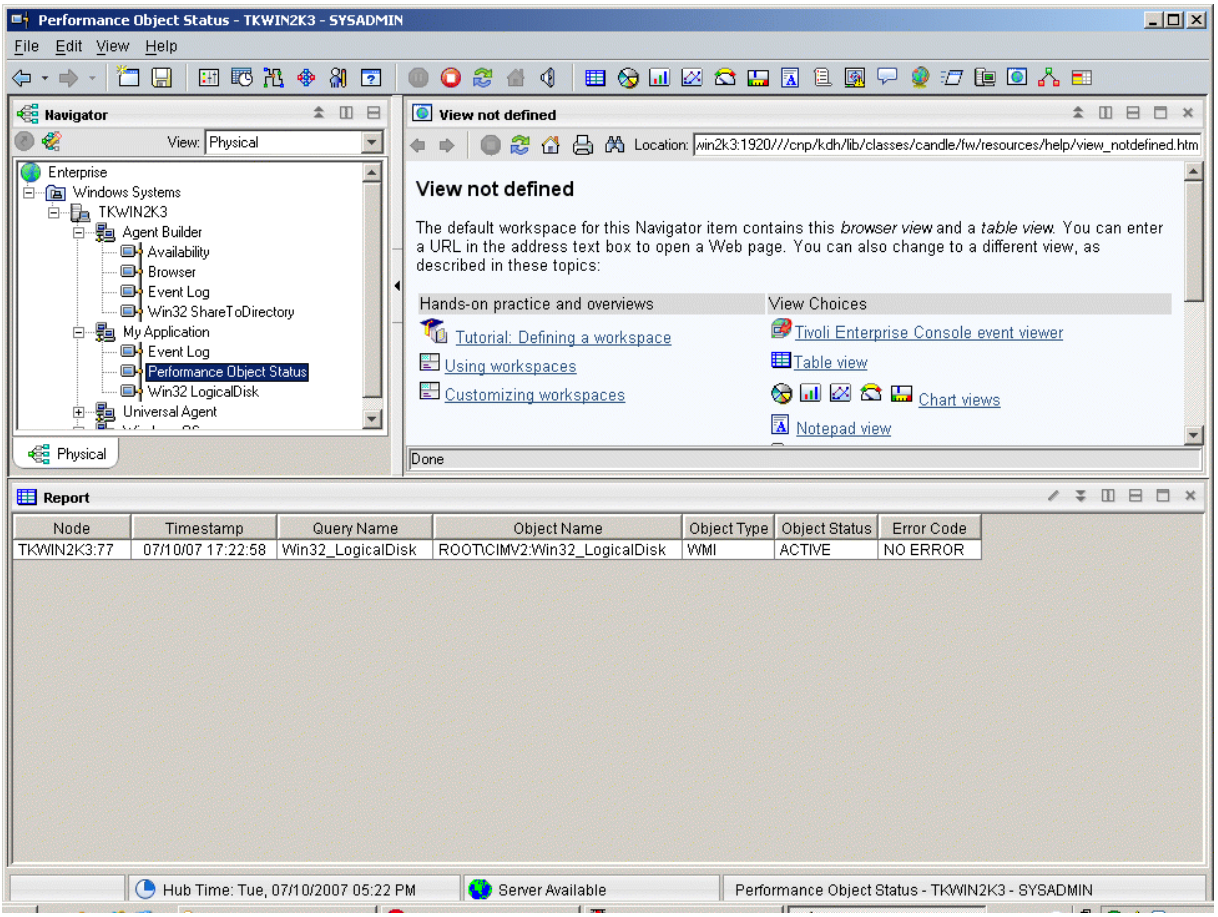


Figura 73. Nodo Estatus de objeto de rendimiento

– Registro de sucesos, si el agente contiene orígenes de datos que producen datos de registro (Figura 74 en la página 1442)

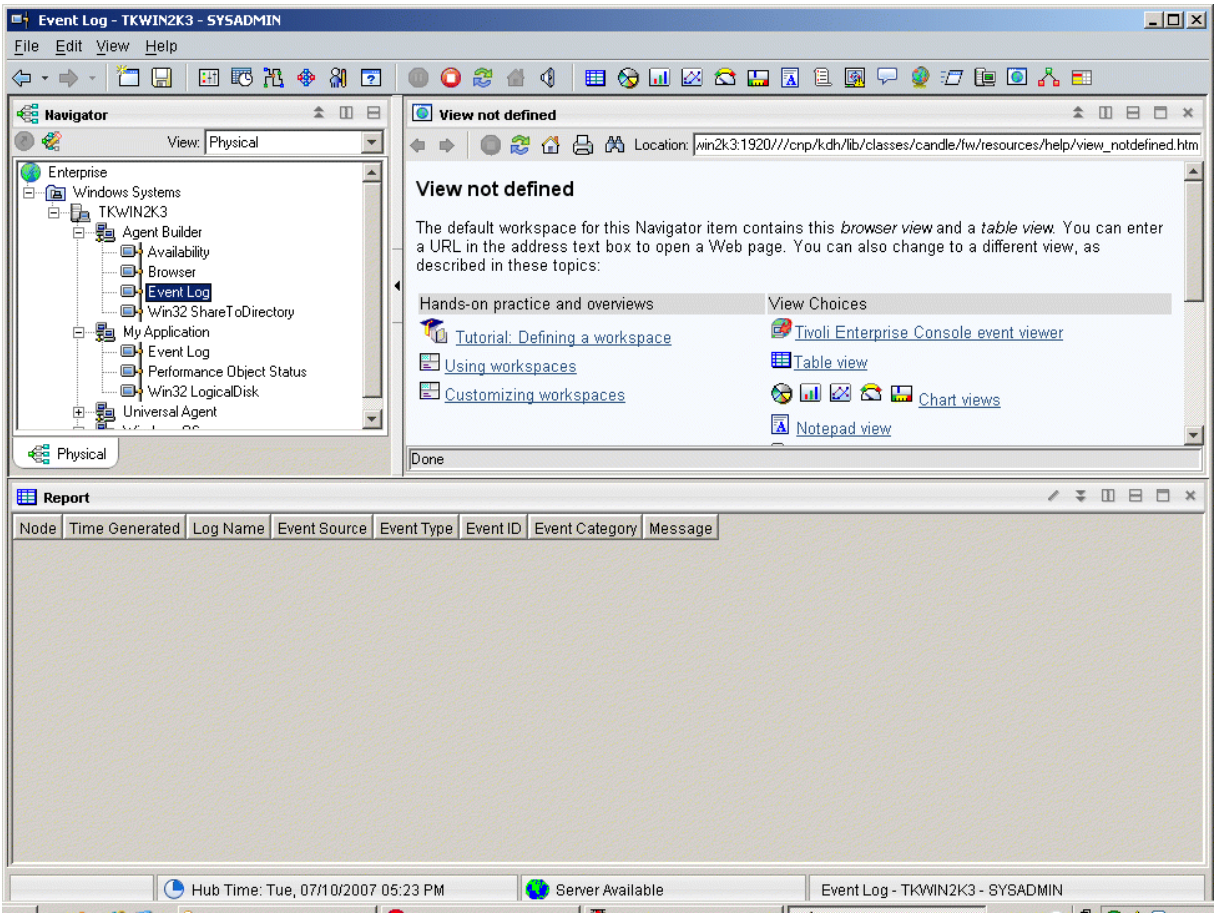


Figura 74. Nodo de registro de sucesos

Consulte “Consulta de atributos” en la página 1457 para ver descripciones de los grupos de atributos y atributos de Agent Builder.

Desinstalación de un agente

Puede eliminar un agente que ha generado el Agent Builder desde un host supervisado.

Acerca de esta tarea

El proceso de desinstalación desinstala sólo el agente del sistema de agente. Este proceso no desinstala ningún otro agente ni ninguna infraestructura de supervisión.

En un entorno IBM Tivoli Monitoring, puede utilizar uno de los procedimientos siguientes para eliminar un agente que ha generado el Agent Builder:

- “Eliminar un agente de Tivoli Monitoring utilizando el Tivoli Enterprise Portal” en la página 1442
- “Eliminar un agente Tivoli Monitoring sin utilizar Tivoli Enterprise Portal” en la página 1443

Tras eliminar el agente utilizando cualquiera de estos procedimientos, bórrelo en Tivoli Enterprise Portal utilizando el procedimiento siguiente: “Borrar un agente de Tivoli Monitoring de Tivoli Enterprise Portal” en la página 1443.

En un entorno IBM Cloud Application Performance Management, utilice el procedimiento siguiente: “Desinstalación de un agente IBM Cloud Application Performance Management” en la página 1443.

Eliminar un agente de Tivoli Monitoring utilizando el Tivoli Enterprise Portal

En un entorno IBM Tivoli Monitoring, puede utilizar el Tivoli Enterprise Portal para eliminar un agente.

Antes de empezar
El agente del sistema operativo debe estar en ejecución para poder eliminar el agente creado.

Procedimiento

Para utilizar el Tivoli Enterprise Portal para eliminar un agente, complete el paso siguiente:

- En el árbol de navegación Tivoli Enterprise Portal, pulse el agente y seleccione **Eliminar**.

Eliminar un agente Tivoli Monitoring sin utilizar Tivoli Enterprise Portal
Si un Tivoli Enterprise Portal no está disponible en el entorno de IBM Tivoli Monitoring, puede utilizar scripts y mandatos del sistema operativo para eliminar un agente.

Procedimiento

Para eliminar un agente que Agent Builder ha generado desde el sistema de destino sin utilizar un Tivoli Enterprise Portal, puede completar cualquiera de los siguientes pasos:

- Windows
  En sistemas Windows, utilice los mandatos:

  ```
  cd ITM_INSTALL/TMAITM6
  kxx_uninstall.vbs ITM_INSTALL
  ```

  donde *xx* es el código de producto para el agente
- Windows
  Como alternativa, en sistemas Windows puede utilizar el mandato `cscript.exe` para ejecutar el script de desinstalación. Este mandato es un analizador de interfaz de línea de mandatos para scripts vbs y no visualiza una ventana; en su lugar, aparece un mensaje en la consola:

  ```
  cd ITM_INSTALL/TMAITM6
  cscript.exe kxx_uninstall.vbs ITM_INSTALL
  ```

- Linux AIX
  En sistemas Linux o UNIX, utilice el archivo `uninstall.sh` que se encuentra en *ITM_INSTALL*`/bin`:

  ```
  uninstall.sh [-f] [-i] [-h ITM_INSTALL] [código_plataforma producto]
  ```

Borrar un agente de Tivoli Monitoring de Tivoli Enterprise Portal
En un entorno de IBM Tivoli Monitoring, tras eliminar el agente, los cambios vacíos de información del agente pueden permanecer en Tivoli Enterprise Portal. Para eliminar los campos, borre el agente de Tivoli Enterprise Portal.

Procedimiento

1. Asegúrese de que el servidor de Tivoli Enterprise Monitoring y el servidor de Tivoli Enterprise Portal estén activos y en ejecución.
2. Inicie sesión en el cliente de Tivoli Enterprise Portal.
3. En la vista Physical Navigator del cliente de Tivoli Enterprise Portal, pulse con el botón derecho del ratón en **Enterprise** y seleccione **Espacio de trabajo** > **Estado de sistema gestionado**.
   Aparecerá el espacio de trabajo Estado de sistemas gestionados.
4. Seleccione todos los sistemas gestionados de IBM Tivoli correspondientes al agente.
5. Pulse con el botón derecho del ratón y seleccione **Borrar entrada fuera de línea**, que borra todas las entradas de la tabla.

Desinstalación de un agente IBM Cloud Application Performance Management
Puede desinstalar el agente desde cualquier sistema supervisado en un entorno de IBM Cloud Application Performance Management.

Procedimiento

1. En el sistema donde se ha instalado el agente, inicie una línea de mandatos y vaya al directorio *dir_instalación*/bin, donde *dir_instalación* es el directorio de instalación de los agentes de supervisión.
2. Si desea desinstalar un agente de supervisión específico, especifique el nombre de script del agente y la opción de desinstalación donde *nombre* es el nombre de script del agente:
   - En sistemas Windows, *nombre*-agent.bat uninstall
   - En sistemas Linux o AIX, ./*nombre*-agent.sh uninstall

Importación de archivos de soporte de aplicaciones

Si se va a utilizar un agente en un entorno IBM Tivoli Monitoring, se pueden incluir situaciones personalizadas, espacios de trabajo, mandatos de actuación y consultas en el paquete de instalación.

Acerca de esta tarea

Para tener una sola imagen de instalación para las situaciones, los espacios de trabajo y el agente, los archivos de las situaciones y espacios de trabajo deben encontrarse en el mismo proyecto que el agente. Agent Builder incluye un asistente para crear los archivos apropiados en el proyecto del agente.

Las definiciones que se asocian con un agente también se pueden incluir en el paquete de instalación. El contenido de estas definiciones es distinto para un agente que se utiliza en un entorno Enterprise Monitoring y en un entorno de supervisor del sistema. Una imagen de agente de Enterprise Monitoring puede incluir situaciones, espacios de trabajo, mandatos de actuación y consultas personalizados. Una imagen de agente supervisor del sistema puede incluir situaciones privadas, definiciones de condiciones de excepción e información de configuración del agente.

Para disponer de un paquete de instalación único que incluya las definiciones apropiadas y el propio agente, los archivos deben estar en el mismo proyecto que el agente. Agent Builder proporciona un asistente para crear los archivos adecuados para una instalación de Enterprise Monitoring. Los archivos para un entorno de agente supervisor del sistema se crean mediante el proceso descrito en el capítulo *Autonomía del agente* de *IBM Tivoli Monitoring: Guía del administrador*. Los archivos resultantes se copian en la raíz del proyecto Eclipse para el agente.

Exportación e importación de archivos para agentes de Tivoli Enterprise Monitoring

Acerca de esta tarea

Después de crear situaciones, espacios de trabajo, consultas y mandatos de actuación en Tivoli Enterprise Portal, puede exportarlos e importarlos a otro entorno de Tivoli Monitoring Versión 6.2. Para obtener más información sobre la creación de situaciones y espacios de trabajo, consulte el “Creación de espacios de trabajo, mandatos de Actuación y situaciones” en la página 1408. Siga estos pasos para extraer las situaciones, los espacios de trabajo, los mandatos de actuación y las consultas:

Procedimiento

1. En el separador **Explorador de proyectos**, pulse con el botón derecho del ratón en la carpeta del proyecto del agente.
2. Seleccione **IBM Corporation** > **Importar archivos de soporte de aplicaciones**.
3. Entre el nombre de host del servidor de Tivoli Enterprise Portal.
4. Entre el nombre de usuario y contraseña para el entorno de Tivoli Monitoring al que se está conectando y pulse **Finalizar**.
5. Si ha definido situaciones para el agente, aparecerá un recuadro de diálogo que lista las situaciones definidas para el agente.

6. Seleccione las situaciones que desea exportar de la lista y pulse **<<** para añadirlas a la tabla de situaciones seleccionadas y pulse **Aceptar**.

   La importación puede tardar unos minutos en llevarse a cabo. Cuando la tarea finalice, verá los archivos SQL en las carpetas apropiadas del proyecto del agente.
7. Si ha definido los mandatos de Actuación para el agente, un diálogo presenta los mandatos de Actuación definidos. Elija los mandatos de actuación que desea exportar de la lista y pulse **>>** para añadirlos a la tabla de actuaciones seleccionadas y pulse **Aceptar**.

   La importación puede tardar unos minutos en llevarse a cabo. Cuando la tarea finalice, verá los archivos SQL en las carpetas apropiadas del proyecto del agente.
8. Si ha definido consultas personalizadas para el agente, un diálogo presenta las consultas definidas. Seleccione las consultas que desea exportar de la lista y pulse **<<** para añadirlas a la tabla de consultas seleccionadas y pulse **Aceptar**.

   La importación puede tardar unos minutos en llevarse a cabo. Cuando la tarea finalice, verá los archivos SQL en las carpetas apropiadas del proyecto del agente. Los espacios de trabajo se importan automáticamente.

Qué hacer a continuación
Vuelva a crear su agente personalizado, instale el agente en el host supervisado e instale el soporte de Tivoli Enterprise Portal.

Exportación e importación de archivos para Tivoli System Monitor Agents

Acerca de esta tarea
Las definiciones del agente supervisor del sistema se encuentran en tres tipos de archivo:

- Las situaciones privadas se definen en un archivo denominado *xx*`_situations.xml`, donde *xx* es el código de dos caracteres del producto
- La información de configuración de las condiciones de excepción se define en un archivo denominado *xx*`_trapcnfg.xml`, donde *xx* es el código de dos caracteres del producto
- Para los agentes que requieran configuración, la configuración se define en un archivo para cada instancia del agente. Cuando el agente es un agente de única instancia, el archivo se denomina *xx*`.cfg`. Cuando el agente es un agente de varias instancias, hay un archivo presente para cada instancia. Los nombres de archivo son *xx_nombre_instancia*`.cfg`, donde *xx* es el código de dos caracteres del producto y *nombre_instancia* es el nombre de la instancia del agente.

Procedimiento

- Cree los archivos utilizando el proceso descrito en el capítulo *Autonomía del agente* de *IBM Tivoli Monitoring: Guía del administrador*. Copie los archivos manualmente en la raíz del directorio del proyecto, o utilice la función de importación de Eclipse para seleccionar los archivos que se deben importar: **Archivo** > **Importar** > **General** > **Sistema de archivos**.

  Estos archivos se incluyen en la imagen del agente y el instalador los instalará.

  Cuando el agente se instala, la instalación:

  – Copia los archivos incluidos en las ubicaciones apropiadas.
  – Las situaciones privadas definidas en el archivo `pc_situations.xml` que se ejecuta en el agente.
  – Las definiciones de condiciones de excepción definidas en `pc_trapcnfg.xml` se utilizan para reenviar condiciones de excepción que se basan en las situaciones.
  – El agente se configura automáticamente y se inicia si:
    - El agente es un agente de una sola instancia sin configuración definida como parte del agente.
    - El agente es un agente de única instancia con la configuración definida como parte del agente y la imagen incluye un archivo `pc.cfg`.

- El agente es un agente de varias instancias (todos los agentes de varias instancias requieren configuración): el instalador inicia una instancia del agente para cada archivo pc_*inst*.cfg.

Filtrado y resumen de sucesos

Un grupo de atributos se define para ser *suceso puro* o *muestreado*. Los grupos de atributos de suceso puro contienen filas de datos que se producen de forma asíncrona. A medida que va llegando cada fila nueva de datos, Tivoli Monitoring la procesa inmediatamente. Los grupos de atributos muestreados recopilan el conjunto actual de filas de datos cada vez que se solicitan los datos. Los siguientes grupos de atributos ilustran la diferencia:

- Se crea un grupo de atributos SNMPEvent que representa todas las condiciones de excepción de SNMP e informa que se envían al agente. Las condiciones de excepción o los informes llegan de forma asíncrona a medida que los envían los sistemas supervisados. A medida que llega cada suceso, se pasa a Tivoli Monitoring.
- Se crea un grupo de atributos Disk para representar información sobre todos los discos de un sistema. La información de disco se recopila de forma periódica. Cada vez que se recopila información de disco, el agente devuelve un número de filas de datos, una por cada disco.

La diferencia entre grupos de atributos de sucesos puros y muestreados afecta a varios aspectos de Tivoli Monitoring. Estos aspectos incluyen: situaciones, datos de almacén y vistas de Tivoli Enterprise Portal.

Cada situación se asigna (o *distribuye*) a uno o varios sistemas gestionados para que se supervise para una determinada condición o un conjunto de condiciones. Cuando la determinación del suceso se debe realizar en función de observaciones que se realizan a intervalos específicos, el suceso se denomina *suceso muestreado*. Cuando el suceso se basa en una aparición espontánea, se denomina *suceso puro*. Por lo tanto, las situaciones para sucesos muestreados tienen un intervalo que está asociado con ellas, mientras que las situaciones para sucesos puros no lo tienen. Otra característica de los sucesos muestreados es que la condición que ha ocasionado el suceso puede cambiar, lo que hace que deje de ser verdadero. Los sucesos puros no se pueden modificar. Por ello, las alertas que se generan para sucesos muestreados pueden pasar de verdaderas a falsas, mientras que un suceso puro sigue siendo verdadero cuando se produce.

Un ejemplo de un suceso muestreado es `número de procesos > 100`. Un suceso se convierte en verdadero cuando el número de procesos supera los 100 y luego se vuelve a convertir en falso cuando su recuento pasa a ser 100 o menos. Una situación que supervisa el `intento de inicio de sesión no válido por parte del usuario` es un suceso puro; el suceso se produce cuando se detecta un intento de inicio de sesión no válido y no se convierte en un suceso falso. Mientras que es posible crear situaciones que se evalúen en un intervalo específico para grupos de atributos muestreados, no lo es para grupos de atributos de sucesos puros.

De forma similar, para datos históricos puede configurar la frecuencia con la que se recopilan los datos muestreados. Sin embargo, cuando se activa la recopilación para datos de sucesos puros, se obtiene cada fila cuando se produce.

Los datos que aparecen en Tivoli Enterprise Portal para los datos muestreados es el conjunto más reciente de filas recopiladas. Los datos que se visualizan para grupos de atributos de sucesos puros son el contenido de una memoria de caché local que el agente mantiene. No coincide necesariamente con los datos que se pasan a Tivoli Monitoring para la evaluación de situación y la recopilación histórica.

Control de sucesos duplicados

Utilice las opciones de filtrado y resumen de sucesos para controlar cómo los sucesos duplicados se envían a Tivoli Monitoring.

Antes de empezar

Para obtener más información sobre el filtrado y resumen de sucesos, consulte el "Filtrado y resumen de sucesos" en la página 1446.

Acerca de esta tarea

Agent Builder define grupos de atributos que representan datos de sucesos como *sucesos puros* en Tivoli Monitoring. Estos grupos de atributos incluyen el archivo de registro, el registro binario de AIX, sucesos de SNMP y notificaciones JMX. Estos grupos de atributos pueden producir varios sucesos duplicados. Puede controlar cómo estos sucesos duplicados se envían a Tivoli Monitoring. Puede activar estos controles para grupos de atributos de archivos de registro, sucesos SNMP y notificaciones JMX en el separador **Información de suceso** de **Propiedades avanzadas de origen de datos** en la ventana **Avanzado**.

Los atributos clave que define en el grupo de atributos determinan si un suceso se trata como un duplicado de otros sucesos. Un suceso duplicado se produce cuando los valores para todos los atributos clave del suceso coinciden con los valores de los mismos atributos de un suceso existente. Cuando el filtro de sucesos y resumen están habilitados, los atributos para las funciones `isSummary`, `occurrenceCount`, `summaryInterval` y `eventThreshold` se añaden automáticamente.

Procedimiento

- En el área **Opciones de filtrado y resumen de sucesos**, seleccione una de estas opciones:
  - **Sin filtrado ni resumen de sucesos**: Envía todos los sucesos sin filtro de sucesos ni resumen. Esta opción es la opción predeterminada.
  - **Filtrar y resumir sucesos**: Crea un registro de resumen para cada suceso con duplicados y cada suceso exclusivo basado en los atributos clave. Seleccione esta opción también para elegir la opción de filtro de sucesos. En el área **Opciones de resumen**, especifique el intervalo de resumen. Puede especificar un valor en segundos o insertar una propiedad de configuración.

    Las opciones de filtro de sucesos son:

    - **Enviar solo sucesos de resumen**: Solo envía los registros de resumen correspondientes al intervalo especificado.
    - **Enviar todos los sucesos**: Envía todos los sucesos y registros de resumen.
    - **Enviar primer suceso**: Para cada suceso, solo envía el primer suceso que se recibe en el intervalo de resumen que se ha especificado y no sucesos duplicados. Esta opción también envía los registros de resumen.
    - **Umbral de sucesos**: Envía un suceso a Tivoli Monitoring cuando el número de sucesos duplicados que se reciben en el intervalo es divisible por el umbral. Por ejemplo, si establece el umbral de sucesos en 5 y recibe menos de cinco duplicados (incluido el primer suceso) en el intervalo, no se envía ningún suceso a Tivoli Monitoring. Si recibe 5, 6, 7, 8 o 9 duplicados, se envía un suceso. Si recibe 10 duplicados, se envían 2 sucesos. En el campo **Umbral de sucesos**, puede especificar un número o insertar una propiedad de configuración. Esta opción también envía los registros de resumen.

Visualización del filtrado y resumen de sucesos en Tivoli Enterprise Portal

Ejemplos de cómo se tratan los datos en función de las opciones de filtrado y resumen de sucesos.

El agente mantiene una memoria caché de los últimos sucesos recibidos. De forma predeterminada, la memoria caché tiene un tamaño de 100. Si habilita el filtrado y resumen de sucesos del agente, se pueden producir diferencias entre el número de sucesos de la memoria caché y el número enviado a IBM Tivoli Monitoring. Los sucesos adicionales de la memoria caché puede que no alcancen el umbral designado para el envío. O puede que tenga menos sucesos en la memoria caché si ha seleccionado la opción **Enviar todos los sucesos**. Si se ha establecido la opción **Enviar todos los sucesos**, se envía un suceso cada vez que se produce un duplicado. Sin embargo, solo una copia del suceso se guarda en la memoria caché, y el número de apariciones se incrementa cada vez que ocurre el suceso. Para ver los sucesos que se envían a IBM Tivoli Monitoring, cree una vista histórica. Para obtener información sobre cómo crear vistas históricas, consulte *Informes históricos* en la Guía del usuario de Tivoli Enterprise Portal. Puede comparar esta vista con la vista de memoria caché en tiempo real en Tivoli Enterprise Portal. También puede utilizar situaciones para hacer la misma comparación.

Los siguientes ejemplos indican cómo se tratan los mismos datos de registro en función de su selección, si la ha hecho, de filtrado y resumen de sucesos. El agente de ejemplo se ha creado para mostrar los distintos comportamientos. Cada grupo de atributos se ha definido de modo que supervise el mismo archivo de registro. En cada ejemplo, se muestra una vista histórica y una vista en tiempo real (memoria caché). Los nombres de los nodos de Tivoli Enterprise Portal reflejan los valores seleccionados. De forma predeterminada, la vista histórica visualiza los sucesos más recientes al final. La vista en tiempo real predeterminada de la memoria caché muestra los sucesos más recientes en primer lugar. En estos ejemplos, la vista histórica muestra la última hora.

A medida que llegan nuevos sucesos, los puede ver en la vista de memoria caché. A medida que llegan duplicados de un suceso, los datos se actualizan en la fila existente. Cuando transcurre un intervalo de resumen, los sucesos existentes se convierten en sucesos de resumen y se envían. Se añaden nuevas filas para el siguiente intervalo de resumen.

La Figura 75 en la página 1449 muestra la vista histórica y la vista de memoria caché si no ha habilitado el filtrado o resumen de sucesos. Ambas vistas muestran los mismos datos, pero en orden inverso. Para visualizar los sucesos correspondientes, la vista histórica se desplaza hacia abajo y la vista de tiempo real (memoria caché) se desplaza hacia arriba.

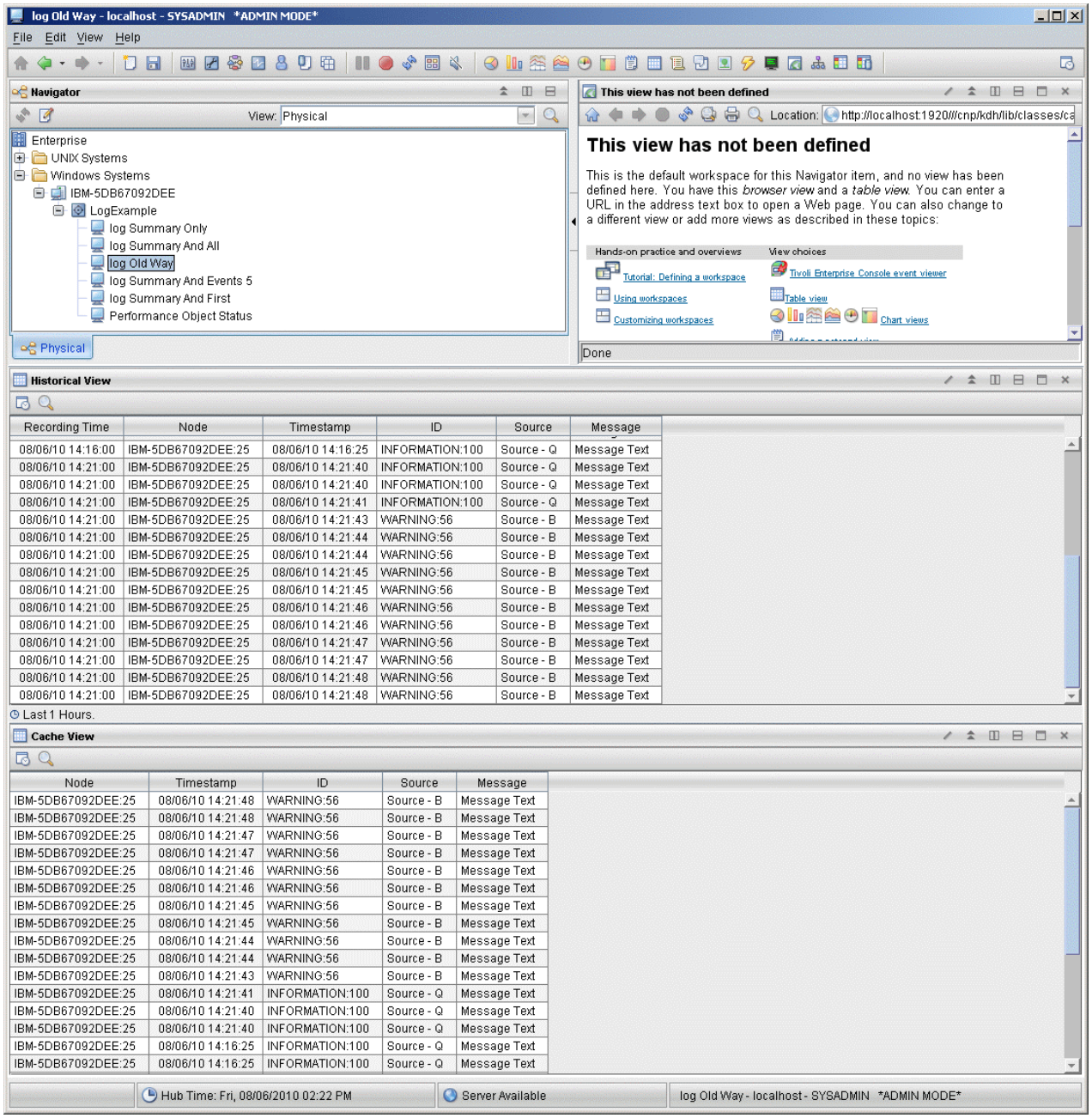


Figura 75. Vista histórica y vista de memoria caché cuando el filtrado o resumen de sucesos no está habilitado

La Figura 76 en la página 1450 muestra la vista histórica y la vista de memoria caché si ha seleccionado la opción **Enviar solo sucesos de resumen** en el separador **Información de suceso**. Los sucesos de resumen se muestran en ambas vistas, pero los sucesos nuevos solo se muestran en la vista en tiempo real (memoria caché).

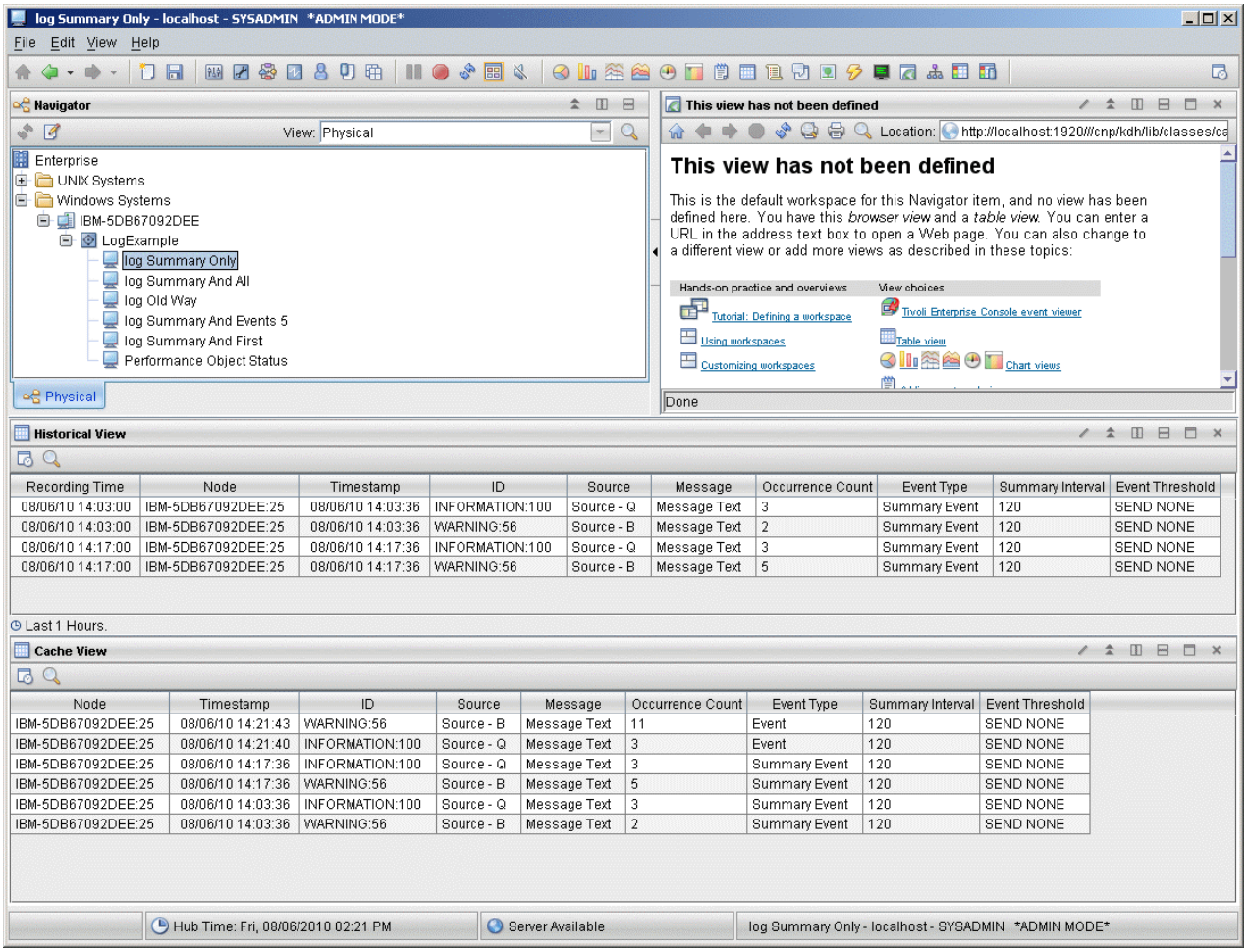


Figura 76. Vista histórica y Vista caché cuando se selecciona ***Enviar solo sucesos de resumen***

La Figura 77 en la página 1451 muestra la vista histórica y la vista de memoria caché si ha seleccionado la opción **Enviar todos sucesos** en el separador **Información de suceso**. Todos los sucesos se muestran en ambas vistas, pero también se ven los sucesos de resumen que se crean al final de cada intervalo. La vista en tiempo real cambia cuando transcurre el intervalo. Los sucesos existentes se convierten en registros de resumen y luego se añaden los sucesos nuevos. La adición de los otros dos atributos de sucesos disponibles que se utilizan para visualizar el intervalo de resumen (120 segundos en este ejemplo) y el umbral *SEND ALL*.

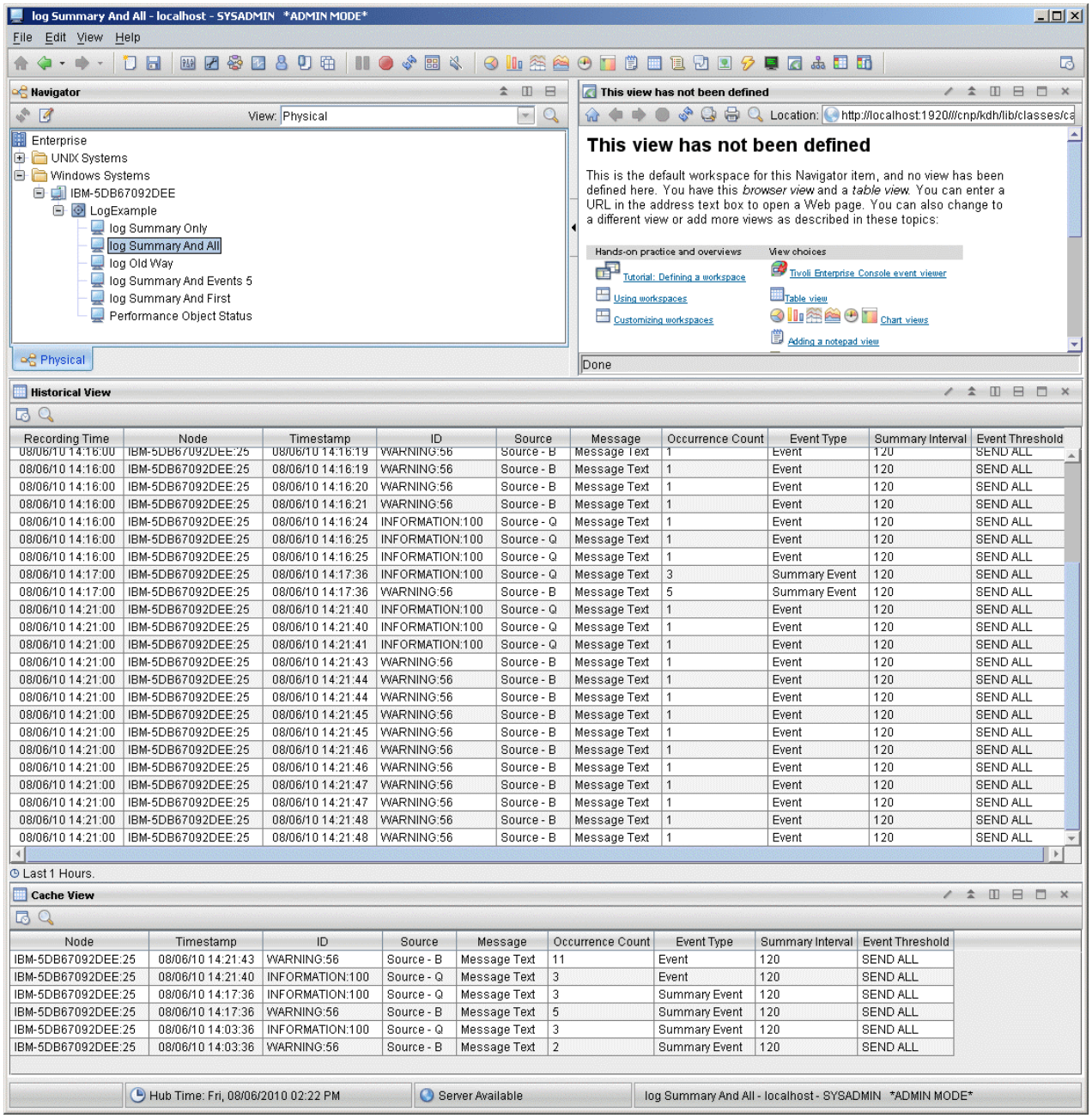


*Figura 77. Vista histórica y Vista caché cuando se selecciona **Enviar todos los sucesos***

La Figura 78 en la página 1452 muestra la vista histórica y la vista de memoria caché si ha seleccionado la opción **Enviar primer suceso** en el separador **Información de suceso**. Los sucesos de resumen se muestran en ambas vistas, pero todos los sucesos nuevos solo se muestran en la vista en tiempo real (memoria caché). Para cada suceso, la vista histórica muestra solo el primer suceso que se recibe en el intervalo y no los sucesos duplicados.

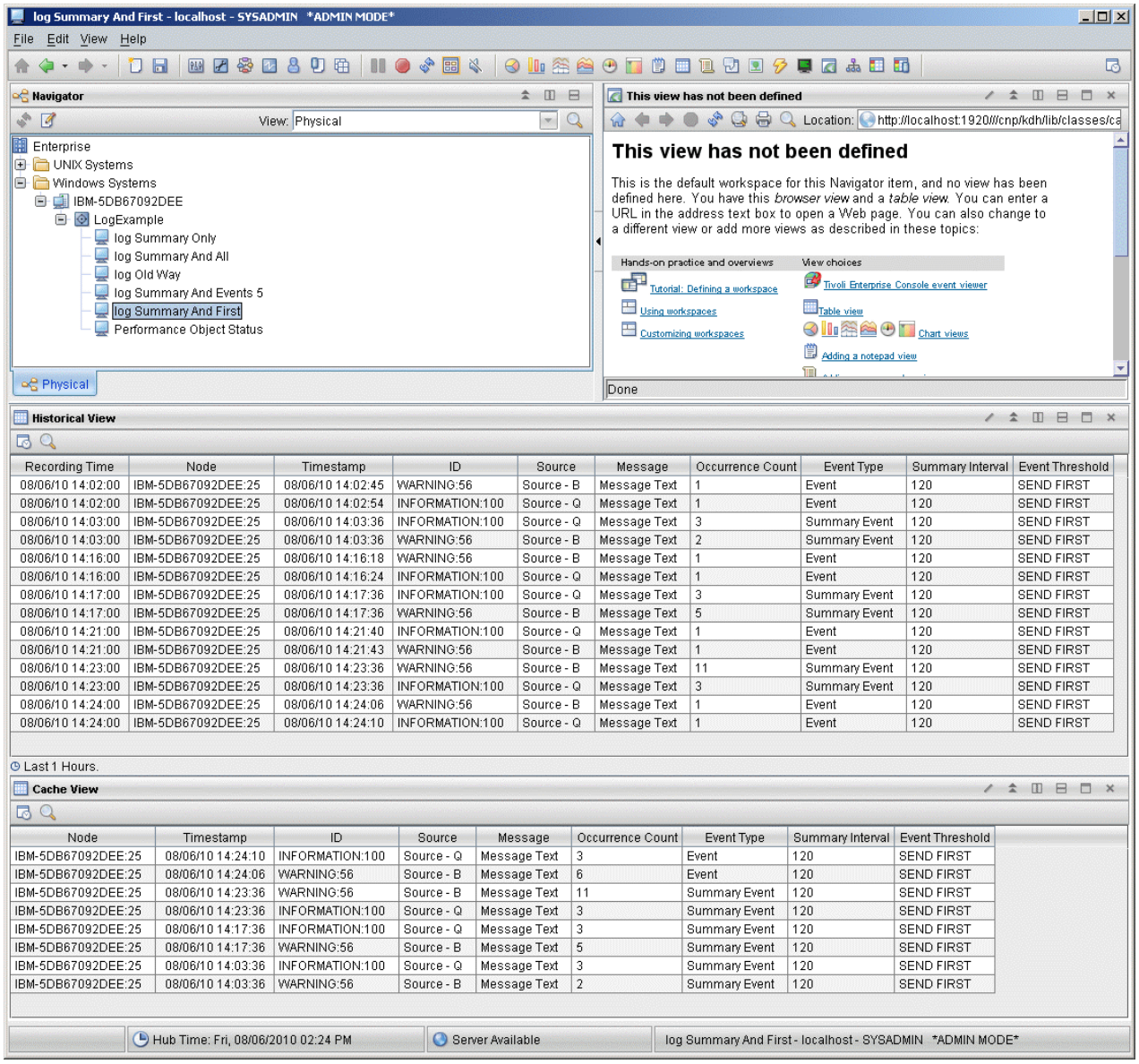


*Figura 78. Vista histórica y vista caché cuando se selecciona **Enviar primer suceso***

La Figura 79 en la página 1453 muestra la vista histórica y la vista de memoria caché si ha seleccionado la opción **Umbral de sucesos** y ha especificado el valor 5. Los sucesos de resumen se visualizan en ambas vistas, pero todos los sucesos nuevos solo se visualizan en la vista de tiempo real (memoria caché). En este ejemplo, se especifica un umbral de 5. La vista histórica visualiza solo un suceso cuando se reciben cinco duplicados de un suceso (incluido el primer suceso) en el intervalo. Si se reciben menos de 5, no se mostrará ningún suceso. Si se reciben 6, 7, 8 o 9 duplicados en el intervalo, se visualiza un suceso. Si se reciben 10 duplicados, aparecerán 2 sucesos.

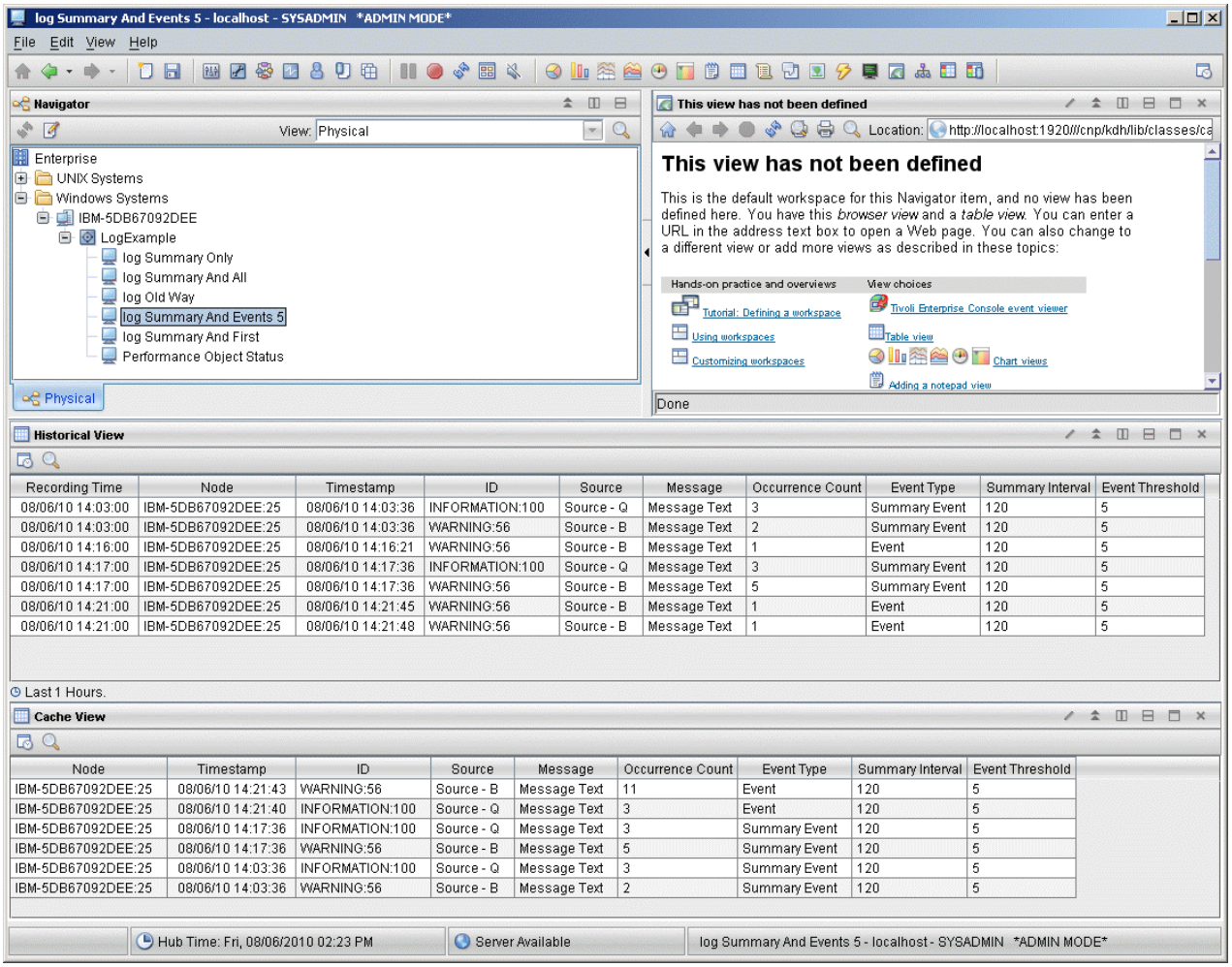


Figura 79. Vista histórica y vista caché cuando se selecciona ***Umbral de suceso***

Conceptos relacionados

"Filtrado y resumen de sucesos" en la página 1446

Resolución de problemas y soporte

Revise la información de resolución de problemas para los problemas que podría experimentar al instalar, configurar o utilizar IBM Agent Builder.

Para obtener ayuda en la resolución de problemas al desarrollar, instalar o utilizar agentes personalizados en el entorno de IBM Cloud Application Performance Management, consulte el Foro de Cloud Application Performance Management en developerWorks. Puede buscar el código "agent_builder", contestar una entrada para hacer una pregunta relacionada, o crear una entrada nueva con su pregunta.

Para obtener información de referencia de registro y mensajes, y ayuda en la resolución de problemas en el entorno de IBM Tivoli Monitoring, consulte Referencia de resolución de problemas de IBM Agent Builder.

Uso compartido de archivo de proyecto

Comparta un proyecto de IBM Tivoli Monitoring Agent.

Procedimiento

1. Obtenga los archivos de las personas con las que desee compartir el proyecto. Necesita el contenido completo del directorio con el mismo nombre que el proyecto del directorio del espacio de trabajo. Por ejemplo, si el directorio de espacio de trabajo es `c:\Documents and Settings\User1\workspace` y desea compartir el proyecto denominado `TestProject`. Debe hacer que el directorio `c:\Documents and Settings\User1\workspace\TestProject` y todo su contenido sea accesible para el sistema.
2. Seleccione **Archivo** > **Importar**.
3. Abra **IBM Tivoli Monitoring**.
4. Seleccione **IBM Tivoli Monitoring Agent** y pulse en **Siguiente**.
5. Escriba la vía de acceso completa para el archivo xml del agente o pulse **Examinar** para navegar hasta el archivo
6. Pulse **Finalizar**.

Resultados
Cuando el asistente finalice, verá el nuevo proyecto de IBM Tivoli Monitoring Agent en el espacio de trabajo.

Compartición de un proyecto del instalador de soluciones

Comparta un proyecto del instalador de soluciones

Procedimiento

1. Obtenga los archivos de las personas con las que desee compartir el proyecto. Debe tener el contenido completo del directorio con el mismo nombre que el proyecto del instalador de soluciones del directorio del espacio de trabajo.
   Por ejemplo, si el directorio del espacio de trabajo es `c:\Documents and Settings\User1\workspace` y desea compartir el proyecto del instalador de soluciones denominado `TestProject Installer`. Debe hacer que el directorio `c:\Documents and Settings\User1\workspace\TestProject Installer` y todo su contenido esté accesible para el sistema.
2. Pulse **Archivo** > **Importar**.
3. Abra **General**.
4. Seleccione **Proyectos existentes en el espacio de trabajo** y pulse **Siguiente**.
5. Escriba la vía de acceso completa para el directorio raíz del proyecto del instalador de soluciones o pulse **Examinar** para navegar hasta el directorio raíz del proyecto de instalador de soluciones. (Ej este ejemplo, el directorio `TestProject Installer`.) El proyecto de dicho directorio se muestra en la lista Proyectos y está seleccionado de manera predeterminada.
6. Opcional: Pulse **Copiar proyectos en el espacio de trabajo**.
7. Pulse **Finalizar**.

Opciones de línea de mandatos

Los mandatos disponibles desde la interfaz de línea de mandatos de Agent Builder (CLI).

Tivoli Monitoring Agent Builder contiene una interfaz de línea de mandatos (CLI) que puede utilizar para generar Tivoli Monitoring Agent sin iniciar la interfaz gráfica de usuario (GUI) de Eclipse. De esta forma, puede generar el agente como parte de una compilación, por ejemplo:

En los sistemas Windows, puede utilizar un archivo por lotes en el directorio siguiente para acceder a la CLI:

```
ubicación_instalación\agenttoolkit.bat
```

En los sistemas UNIX y Linux, puede utilizar un script en el directorio siguiente para acceder a la CLI:

```
ubicación_instalación/agenttoolkit.sh
```

Los mandatos descritos en esta documentación están formateados paras sistemas Windows, que utilizan la barra inclinada invertida (\) para las vías de acceso de directorio.

Para sistemas UNIX® o Linux®, utilice los mismos mandatos que para sistemas Windows, con los siguientes cambios:

- Utilice una barra inclinada (/) para vías de acceso de directorio en lugar de una barra inclinada invertida (\).
- Utilice el script `agenttoolkit.sh` en lugar del script `agenttoolkit.bat`.

Mandatos

La Tabla 300 en la página 1455 lista el nombre y la finalidad de cada opción de mandato para el mandato text:

Tabla 300. Tabla de consulta rápida de mandatos

Mandato	Finalidad
generatelocal	Carga y valida el archivo `itm_toolkit_agent.xml` y genera los archivos que ejecutan Tivoli Monitoring Agent. La instalación se realiza en un entorno local de Tivoli Monitoring.
generatemappingfile	Crea el archivo de la correlación de modelos de recursos personalizados de puertos de IBM Tivoli Monitoring v5.x con agentes de IBM Tivoli Monitoring v6
generatezip	Genera un archivo comprimido denominado *productcode*`.zip` o *productcode*`.tgz`.

Las descripciones de mandatos a los que se hace referencia desde la tablas describen cómo se deben ejecutar los mandatos e incluye la siguiente información:

Finalidad
Describe la finalidad del mandato.

Formato
Especifica la sintaxis que se escribe en la línea de mandatos. La sintaxis contiene el nombre del mandato y una lista de sus parámetros. A continuación del nombre del mandato se incluye una definición de cada uno de sus parámetros.

Ejemplos
El ejemplo del mandato contiene una descripción breve del ejemplo y un ejemplo de la sintaxis.

Uso
Proporciona una explicación del mandato y de su finalidad.

Comentarios
Proporciona mandatos o texto que le pueden suministrar más información.

Mandato: `generatelocal`

Utilice este mandato para cargar y validar el XML y para generar archivos para ejecutar Tivoli Monitoring Agent.

Finalidad

Carga y valida el archivo `itm_toolkit_agent.xml` y genera los archivos para ejecutar Tivoli Monitoring Agent. La instalación se realiza en un entorno local de Tivoli Monitoring.

Formato

En los sistemas Windows:

```
ubicación_instalación\agenttoolkit.bat  dir_proyecto -generatelocal dir_instalación_itm
```

donde:

ubicación_instalación
Directorio en el que está instalado Agent Builder

dir_proyecto
Nombre del directorio que contiene el archivo `itm_toolkit_agent.xml`

dir_instalación_itm
Ubicación en la que Tivoli Monitoring está instalado (por ejemplo `c:\IBM\ITM`)

Ejemplos

En el ejemplo siguiente correspondiente a Windows, se valida la definición de agente en `C:\ABCAgent` y se generan los archivos necesarios para ejecutar ABCAgent en `C:\IBM\ITM`:

```
ubicación_instalación\agenttoolkit.bat C:\ABCAgent -generatelocal C:\IBM\ITM
```

Mandato: `generatemappingfile`

Utilice este mandato para migrar los modelos de recursos personalizados de IBM Tivoli Monitoring v5.x a agentes de IBM Tivoli Monitoring v6.

Finalidad

Este mandato crea el archivo de correlación para migrar modelos de recursos personalizados de IBM Tivoli Monitoring v5.x a agentes de IBM Tivoli Monitoring v6.

Formato

En los sistemas Windows:

```
ubicación_instalación\agenttoolkit.bat dir_proyecto -generatemappingfile dir_salida
   lista_interp_itm5
```

Donde:

ubicación_instalación
Directorio en el que está instalado Agent Builder

dir_proyecto
Nombre del directorio que contiene `itm_toolkit_agent.xml`

dir_salida
Nombre del directorio donde se escribe el archivo de correlación.

lista_interp_itm5
Lista separada por comas de los sistemas operativos de ITM 5x en los cuales se ejecutó el modelo de recurso personalizado. Se permiten los siguientes valores:

- `aix4-r1`
- `hpux10`
- `linux-ix86`
- `linux-ppc`
- `linux-s390`
- `os2-ix86`
- `os400`

- solaris2
- solaris2-ix86
- w32-ix86

Ejemplos

Para sistemas Windows

```
ubicación_instalación\agenttoolkit.bat c:\ABCAgent -generatemappingfile c:\output
   linux-ix86,linux-ppc,linux-s390
```

Mandato: generatezip

Utilice este mandato para cargar y validar el XML y para generar un archivo comprimido que se puede utilizar para instalar el agente en otro sistema.

Finalidad

Carga y valida el archivo itm_toolkit_agent.xml y genera un archivo comprimido denominado *productcode*.zip o *productcode*.tgz. El archivo comprimido generado se puede utilizar para instalar el agente en otro sistema. Según el entorno, se pueden generar ambos tipos de archivo.

Formato

En los sistemas Windows:

```
ubicación_instalación\agenttoolkit.bat  dir_proyecto -generatezip dir_salida
```

Donde:

dir_proyecto
Nombre de un directorio que contiene el archivo itm_toolkit_agent.xml

dir_salida
Nombre del directorio donde se escribe el archivo comprimido.

Ejemplos

En el ejemplo siguiente correspondiente a Windows, la definición de agente en C:\ABCAgent se valida y un archivo comprimido que contiene los archivos necesarios para ejecutar ABCAgent se genera en C:\Output:

```
ubicación_instalación\agenttoolkit.bat\ C:\ABCAgent -generatezip C:\Output
```

Consulta de atributos

Contiene descripciones de los atributos para cada grupo generado de atributos incluido en Agent Builder.

Nodo de disponibilidad

El grupo de atributos de disponibilidad contiene datos de disponibilidad para la aplicación.

La tabla proporciona un formato común para representar la disponibilidad de la aplicación, que incluye información relevante para tres aspectos de una aplicación: servicios (solo Windows), procesos y códigos de retorno de mandato.

La lista siguiente contiene información acerca de todos los atributos que componen el grupo de atributos de Disponibilidad:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se han recopilado los datos.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo Componente de aplicación: este atributo es un atributo clave

Descripción
Nombre descriptivo de una parte de la aplicación

Tipo
Serie

Nombres

Nombre de atributo
Componente_aplicación

Nombre de columna
COMPONENT

Atributo Nombre

Descripción
El nombre del proceso, el servicio o la prueba funcional. Este nombre coincide con el nombre del ejecutable del proceso, el nombre abreviado del servicio o el nombre del proceso utilizado para probar la aplicación.

Tipo
Serie

Nombres

Nombre de atributo
Nombre

Nombre de columna
NAME

Atributo Estatus

Descripción
Estatus del componente de aplicación.

- Para los proceso, los valores son ABAJO, ARRIBA, AVISO o DATOS DE PROCESO NO DISPONIBLES. DATOS DE PROCESO NO DISPONIBLES se visualiza para un proceso cuando el proceso coincidente está ejecutándose pero no se puede recopilar la información de utilización de recursos para ese proceso.
- Para los servicios, los valores son ARRIBA, ABAJO o DESCONOCIDO. DESCONOCIDO se visualiza cuando el servicio no está instalado.
- Para los códigos de retorno de mandatos, los valores son CORRECTO o INCORRECTO.

Tipo
Serie

Nombres

Nombre de atributo
Estatus

Nombre de columna
STATUS

Atributo Nombre completo

Descripción
Nombre completo del proceso que incluye información que depende del proceso. El nombre puede incluir la vía de acceso completa si el proceso se ha iniciado de esta manera. El nombre también puede incluir una vía de acceso parcial o incluso una vía de acceso cambiada por el proceso.

Tipo
Serie

Nombres

Nombre de atributo
Nombre_completo

Nombre de columna
FULLNAME

Atributo Tipo

Descripción
Identifica el tipo del componente de aplicación. Los componentes son los procesos, los servicios o los códigos de retorno de mandato.

Tipo
Entero (indicador)

Nombres

Nombre de atributo
Tipo

Nombre de columna
TYPE

Atributo Tamaño virtual

Descripción
Tamaño virtual (en MB) del proceso

Tipo
Entero (indicador)

Nombres

Nombre de atributo
Virtual_Size

Nombre de columna
VIRTSIZE

Atributo Errores de página por segundo

Descripción
Tasa de errores de página del proceso medida en errores por segundo. Este valor contiene solo datos válidos para procesos.

Tipo
Entero (indicador)

Nombres

Nombre de atributo
Errores_página_por_seg

Nombre de columna
PAGEFAULTS

Atributo Tamaño de conjunto de trabajo

Descripción
Tamaño del conjunto de trabajo del proceso en MB. Este valor contiene solo datos válidos para procesos.

Tipo
Entero (indicador)

Nombres

Nombre de atributo
Tamaño_conjunto_trabajo

Nombre de columna
WORKSET

Atributo Recuento de hebras

Descripción
Número de hebras que este proceso ha asignado actualmente. Este valor contiene solo datos válidos para procesos.

Tipo
Entero (indicador)

Nombres

Nombre de atributo
Thread_Count

Nombre de columna
THREADS

Atributo PID

Descripción
ID de proceso asociado al proceso. Este valor contiene solo datos válidos para procesos.

Tipo
Entero (indicador)

Nombres

Nombre de atributo
PID

Nombre de columna
PID

Atributo Porcentaje de tiempo con privilegios

Descripción
Porcentaje del tiempo de procesador disponible que el proceso utiliza para la operación privilegiada

Tipo
Entero (indicador)

Nombres

Nombre de atributo
Porcentaje_tiempo_privilegios

Nombre de columna
PERCPRIV

Atributo Porcentaje de tiempo en modalidad de usuario

Descripción
Porcentaje del tiempo de procesador disponible que el proceso utiliza para la operación en modalidad de usuario

Tipo
Entero (indicador)

Nombres

Nombre de atributo
Porcentaje_tiempo_modalidad_usuario

Nombre de columna
PERCUSER

Atributo Porcentaje de tiempo de procesador

Descripción
Porcentaje del tiempo transcurrido durante el cual el proceso ha utilizado el procesador para ejecutar instrucciones

Tipo
Entero (indicador)

Nombres

Nombre de atributo
Porcentaje_tiempo_procesador

Nombre de columna
PERCPROC

Atributo Línea de mandatos

Descripción
Nombre de programa y cualquier argumento especificado en la línea de mandatos al iniciarse el proceso. Este atributo tiene el valor *N/A* si se ejecuta una prueba de Servicio o Funcionalidad.

Tipo
Serie

Nombres

Nombre de atributo
Línea_mandatos

Nombre de columna
CMDLINE

Atributo Estatus de prueba de funcionalidad

Descripción
Código de retorno de la prueba de funcionalidad. Cuando la aplicación supervisada se ejecuta correctamente, se devuelve SUCCESS. Se devuelve NOT_RUNNING cuando la aplicación no se ejecuta correctamente. Se devuelve N/A cuando la fila no representa una prueba de funcionalidad.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal, el almacén y las consultas devuelven los números. Los valores definidos son: N/A(1), SUCCESS (0), GENERAL_ERROR (2), WARNING (3), NOT_RUNNING (4), DEPENDENT_NOT_RUNNING (5), ALREADY_RUNNING (6), PREREQ_NOT_RUNNING (7), TIMED_OUT (8), DOESNT_EXIST (9), UNKNOWN (10), DEPENDENT_STILL_RUNNING (11) o INSUFFICIENT_USER_AUTHORITY (12). Cualquier otro valor visualiza el valor numérico en Tivoli Enterprise Portal.

Nombres

Nombre de atributo
Estatus_prueba_funcionalidad

Nombre de columna
FUNCSTATUS

Atributo Mensaje de prueba de funcionalidad

Descripción
Mensaje de texto que corresponde al estatus de la prueba de funcionalidad. Este atributo solo es válido para códigos de retorno de mandato.

Tipo
Serie

Nombres

Nombre de atributo
Mensaje_prueba_funcionalidad

Nombre de columna
FUNCMSG

Nodo Estatus de objeto de rendimiento

Utilice el grupo de atributos Estatus de objeto de rendimiento para ver el estatus de todos los grupos de atributos que componen el agente. Cada uno de los grupos de atributos se representa mediante una fila en esta tabla u otro tipo de vista. El estatus de un grupo de atributos refleja el resultado del último intento de recopilación de datos, o el suceso de recepción de datos, para el grupo de atributos. Al comprobar la información de estado, puede ver si el agente opera correctamente. Cuando el agente no recopila datos, pero los recibe (datos de sucesos), los atributos que están relacionados con los datos muestreados no contienen datos útiles. Solo los siete primeros atributos que se listan son relevantes para los datos de suceso.

Grupo histórico
Este grupo de atributos es elegible para utilizarse con Tivoli Data Warehouse.

Descripciones de atributo
La lista siguiente contiene información acerca de todos los atributos que componen el grupo de atributos Estatus de objetos de rendimiento:

Atributo Nodo: este atributo es un atributo clave.

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Nombre de almacén
NODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Nombre de almacén
TIMESTAMP

Atributo Nombre de consulta: este atributo es un atributo clave.

Descripción
Nombre del grupo de atributos.

Tipo
Serie

Nombre de almacén
QUERY_NAME o ATTRGRP

Atributo Nombre de objeto

Descripción
Nombre del objeto de rendimiento.

Tipo
Serie

Nombre de almacén
OBJECT_NAME u OBJNAME

Atributo Tipo de objeto

Descripción
Tipo del objeto de rendimiento.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los valores que se muestran entre paréntesis. Están definidos los valores siguientes:

- WMI (0)
- PERFMON (1)
- GRUPO DE ASOCIACIONES WMI (2)
- JMX (3)
- SNMP (4)
- MANDATO DE SHELL (5)
- GRUPOS UNIDOS (6)
- CIMOM (7)
- PERSONALIZADO (8)
- DATOS DE RESUMEN (9)
- DATOS REMOTOS DE WMI (10)

- ARCHIVO DE REGISTRO (11)
- JDBC (12)
- DESCUBRIMIENTO DE CONFIGURACIÓN (13)
- REGISTRO DE SUCESOS DE NT (14)
- FILTRO (15)
- SUCESO SNMP (16)
- PING (17)
- DATOS DE DIRECTOR (18)
- SUCESO DE DIRECTOR (19)
- MANDATO DE SHELL REMOTO DE SSH (20)

Cualquier otro valor es el valor devuelto por el agente en el Tivoli Enterprise Portal.

Nombre de almacén
OBJECT_TYPE u OBJTYPE

Atributo Estatus del objeto

Descripción
Estado del objeto de rendimiento.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los valores que se muestran entre paréntesis. Están definidos los valores siguientes:

- ACTIVO (0)
- INACTIVO (1)

Cualquier otro valor es el valor devuelto por el agente en el Tivoli Enterprise Portal.

Nombre de almacén
OBJECT_STATUS u OBJSTTS

Atributo Código de error

Descripción
Código de error que está asociado con la consulta.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los valores que se muestran entre paréntesis. Están definidos los valores siguientes:

- NINGÚN ERROR (0)
- ERROR GENERAL (1)
- OBJETO NO ENCONTRADO (2)
- CONTADOR NO ENCONTRADO (3)
- ERROR DE ESPACIO DE NOMBRES (4)
- OBJETO NO DISPONIBLE ACTUALMENTE (5)
- ANOMALÍA DE INICIALIZACIÓN DE BIBLIOTECA COM (6)
- ANOMALÍA DE INICIALIZACIÓN DE SEGURIDAD (7)
- ANOMALÍA DE SEGURIDAD DEL PROXY (9)
- NINGUNA INSTANCIA DEVUELTA (10)
- CONSULTA DE ASOCIADOR ANÓMALA (11)
- CONSULTA DE REFERENCIA ANÓMALA (12)

- NINGUNA RESPUESTA RECIBIDA (13)
- NO SE ENCUENTRA CONSULTA UNIDA (14)
- NO SE ENCUENTRA ATRIBUTO DE UNIÓN EN RESULTADOS DE CONSULTA 1 (15)
- NO SE ENCUENTRA ATRIBUTO DE UNIÓN EN RESULTADOS DE CONSULTA 2 (16)
- CONSULTA 1 NO ES ÚNICA (17)
- CONSULTA 2 NO ES ÚNICA (18)
- NINGUNA INSTANCIA DEVUELTA EN CONSULTA 1 (19)
- NINGUNA INSTANCIA DEVUELTA EN CONSULTA 2 (20)
- NO SE ENCUENTRA CONSULTA DE SUMARIZACIÓN (21)
- NO SE ENCUENTRA ATRIBUTO DE SUMARIZACIÓN (22)
- ARCHIVO FUERA DE LÍNEA (23)
- SIN NOMBRE DE HOST (24)
- FALTA BIBLIOTECA (25)
- NO COINCIDENCIA RECUENTO ATRIBUTOS (26)
- NO COINCIDENCIA NOMBRE ATRIBUTO (27)
- PROVEEDOR DE DATOS COMÚN NO INICIADO (28)
- ERROR REGISTRO DEVOLUCIÓN LLAMADA (29)
- ERROR DE CARGA DE MDL (30)
- LA AUTENTICACIÓN HA FALLADO (31)
- NO SE PUEDE RESOLVER NOMBRE DE HOST (32)
- SUBNODO NO DISPONIBLE (33)
- SUBNODO NO ENCONTRADO EN LA CONFIGURACIÓN (34)
- ERROR DE ATRIBUTO (35)
- ERROR DE VÍA DE ACCESO DE CLASE (36)
- ANOMALÍA DE CONEXIÓN (37)
- ERROR DE SINTAXIS DE FILTRO (38)
- FALTA NOMBRE DE ARCHIVO (39)
- ERROR DE CONSULTA SQL (40)
- ERROR DE CONSULTA DE FILTRO SQL (41)
- ERROR DE CONSULTA DE BD SQL (42)
- ERROR DE CONSULTA DE FILTRO DE BD SQL (43)
- ERROR DE APERTURA DE PUERTO (44)
- ACCESO DENEGADO (45)
- TIEMPO DE ESPERA EXCEDIDO (46)
- NO IMPLEMENTADO (47)
- SOLICITADO UN VALOR ERRÓNEO (48)
- RESPUESTA DEMASIADO GRANDE (49)
- GENERAL RESPONSE ERROR (50)
- DEVOLUCIÓN DE SCRIPT DISTINTA DE CERO (51)
- SCRIPT NO ENCONTRADO (52)
- ERROR DE INICIO DE SCRIPT (53)
- EL ARCHIVO DE CONFIGURACIÓN NO EXISTE (54)
- ACCESO DENEGADO AL ARCHIVO DE CONFIGURACIÓN (55)

- ARCHIVO DE CONFIGURACIÓN NO VÁLIDO (56)
- HA FALLADO LA INICIALIZACIÓN DE EIF (57)
- NO SE PUEDE ABRIR EL ARCHIVO DE FORMATO (58)
- ERROR DE SINTAXIS DEL ARCHIVO DE FORMATO (59)
- HOST REMOTO NO DISPONIBLE (60)
- EL REGISTRO DE SUCESOS NO EXISTE (61)
- EL ARCHIVO DE PING NO EXISTE (62)
- NO HAY ARCHIVOS DE DISPOSITIVO PING (63)
- FALTA EL ARCHIVO DE LISTA DE DISPOSITIVOS PING (64)
- FALTA CONTRASEÑA DE SNMP (65)
- INHABILITADO (66)
- ARCHIVO DE URL NO ENCONTRADO (67)
- ERROR DE ANÁLISIS DE XML (68)
- NO INICIALIZADO (69)
- LOS ZÓCALOS DE ICMP HAN FALLADO (70)

Cualquier otro valor es el valor devuelto por el agente en el Tivoli Enterprise Portal.

Nombre de almacén
ERROR_CODE o ERRCODE

Atributo Último inicio de recopilación

Descripción
Hora más reciente en que se ha iniciado una recopilación de datos de este grupo.

Tipo
Indicación de fecha y hora con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los valores que se muestran entre paréntesis. Están definidos los valores siguientes:

- NO RECOPILADA (0691231190000000)
- NO RECOPILADA (0000000000000001)

Cualquier otro valor es el valor devuelto por el agente en el Tivoli Enterprise Portal.

Nombre de almacén
LAST_COLLECTION_START o COLSTRT

Atributo Última recopilación finalizada

Descripción
Hora más reciente en que ha finalizado una recopilación de datos de este grupo.

Tipo
Indicación de fecha y hora con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los valores que se muestran entre paréntesis. Están definidos los valores siguientes:

- NO RECOPILADA (0691231190000000)
- NO RECOPILADA (0000000000000001)

Cualquier otro valor es el valor devuelto por el agente en el Tivoli Enterprise Portal.

Nombre de almacén
LAST_COLLECTION_FINISHED o COLFINI

Atributo Duración de última recopilación

Descripción
Duración de la recopilación de datos completada más recientemente de este grupo en segundos.

Tipo
Número real (contador de 32 bits) con dos posiciones decimales de precisión

Nombre de almacén
LAST_COLLECTION_DURATION o COLDURA

Atributo Promedio de duración de recopilación

Descripción
Duración media de todas las recopilaciones de datos de este grupo en segundos.

Tipo
Número real (contador de 32 bits) con dos posiciones decimales de precisión con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los valores que se muestran entre paréntesis. Están definidos los valores siguientes:

- `SIN DATOS (-100)`

Cualquier otro valor es el valor devuelto por el agente en el Tivoli Enterprise Portal.

Nombre de almacén
AVERAGE_COLLECTION_DURATION o COLAVGD

Atributo Intervalo de renovación

Descripción
Intervalo durante el cual se ha renovado este grupo en segundos.

Tipo
Entero (contador de 32 bits)

Nombre de almacén
REFRESH_INTERVAL o REFRINT

Atributo Número de recopilaciones

Descripción
Número de veces que se ha recopilado este grupo desde el inicio del agente.

Tipo
Entero (contador de 32 bits)

Nombre de almacén
NUMBER_OF_COLLECTIONS o NUMCOLL

Atributo Aciertos de memoria caché

Descripción
Número de veces que se satisface una solicitud de datos externa para este grupo desde la memoria caché.

Tipo
Entero (contador de 32 bits)

Nombre de almacén
CACHE_HITS o CACHEHT

Atributo Desaciertos de memoria caché

Descripción
Número de veces que una solicitud de datos externa para este grupo no estaba disponible en la memoria caché.

Tipo
Entero (contador de 32 bits)

Nombre de almacén
CACHE_MISSES o CACHEMS

Atributo Porcentaje de aciertos de memoria caché

Descripción
Porcentaje de solicitudes de datos externas para este grupo que se satisfacen desde la memoria caché.

Tipo
Número real (contador de 32 bits) con dos posiciones decimales de precisión

Nombre de almacén
CACHE_HIT_PERCENT o CACHPCT

Atributo Intervalos omitidos

Descripción
El número de veces que se omitió una recopilación de datos en segundo plano porque la recopilación anterior aún estaba en ejecución cuando estaba previsto iniciar la siguiente.

Tipo
Entero (contador de 32 bits)

Nombre de almacén
INTERVALS_SKIPPED o INTSKIP

Grupo de atributos Estatus de agrupación de hebras

El grupo de atributos Estado de agrupación de hebras contiene información que refleja el estado de la agrupación de hebras interna que se utiliza para recopilar datos asíncronamente.

A continuación se ofrece una lista de los atributos de este grupo de atributos. El nombre en negrita muestra cómo se visualiza el atributo en Tivoli Enterprise Portal.

La lista siguiente contiene información sobre todos los atributos del grupo de atributos Estatus de agrupación de hebras:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora recopilada del sistema de agente cuando se creó la fila de datos y se envió del agente al servidor de Tivoli Enterprise Monitoring. O se ha almacenado con fines históricos. Representa el huso horario local del sistema agente.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo Tamaño de agrupación de hebras

Descripción
Número de hebras que existen actualmente en la agrupación de hebras.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Size

Nombre de columna
THPSIZE

Atributo Tamaño máximo de agrupación de hebras

Descripción
Número máximo de hebras que se permite que existan en la agrupación de hebras.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Max_Size

Nombre de columna
TPMAXSZ

Atributo Hebras activas de agrupación de hebras

Descripción
Número de hebras de la agrupación de hebras actualmente activas que realizan un trabajo.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Active_Threads

Nombre de columna
TPACTTH

Atributo Promedio de hebras activas de agrupación de hebras

Descripción
Número medio de hebras de la agrupación de hebras simultáneamente activas que realizan un trabajo.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Avg_Active_Threads

Nombre de columna
TPAVGAT

Atributo Mínimo de hebras activas de agrupación de hebras

Descripción
Número mínimo de hebras de la agrupación de hebras simultáneamente activas que realizan un trabajo.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Min_Active_Threads

Nombre de columna
TPMINAT

Atributo Máximo de hebras activas de agrupación de hebras

Descripción
Número máximo de hebras de la agrupación de hebras simultáneamente activas que realizan un trabajo.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Max_Active_Threads

Nombre de columna
TPMAXAT

Atributo Longitud de cola de agrupación de hebras

Descripción
Número de trabajos actualmente en espera en la cola de agrupación de hebras.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Queue_Length

Nombre de columna
TPQLGTH

Atributo Promedio de longitud de cola de agrupación de hebras

Descripción
Promedio de longitud de la cola de agrupación de hebras durante esta ejecución.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Avg_Queue_Length

Nombre de columna
TPAVGQL

Atributo Longitud de cola mínima de agrupación de hebras

Descripción
Longitud mínima que ha alcanzado la cola de agrupación de hebras.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Min_Queue_Length

Nombre de columna
TPMINQL

Atributo Longitud de cola máxima de agrupación de hebras

Descripción
Longitud de hora punta que ha alcanzado la cola de agrupación de hebras.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Max_Queue_Length

Nombre de columna
TPMAXQL

Atributo Promedio de espera de trabajo de agrupación de hebras

Descripción
Promedio de tiempo que un trabajo pasa en espera en la cola de agrupación de hebras.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Avg_Job_Wait

Nombre de columna
TPAVJBW

Atributo Total de trabajos de agrupación de hebras

Descripción
Número de trabajos completados por todas las hebras de la agrupación desde el inicio del agente.

Tipo
Entero

Nombres

Nombre de atributo
Thread_Pool_Total_Jobs

Nombre de columna
TPTJOBS

Nodo de atributo de registro de sucesos

El grupo de atributos de registro de sucesos contiene las entradas recientes del registro de sucesos que pertenecen a la aplicación.

De forma predeterminada, el agente sólo muestra sucesos que se producen después de iniciar el agente. Los sucesos se eliminan de la vista Registro de sucesos una hora después de producirse.

La lista siguiente contiene información sobre todos los atributos del grupo de atributos Registro de sucesos:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Nombre de registro

Descripción
Registro de sucesos: registro de la aplicación, del sistema, de seguridad o de una aplicación específica

Tipo
Serie

Nombres

Nombre de atributo
Nombre_registro

Nombre de columna
LOGNAME

Atributo Origen de sucesos

Descripción
Origen del suceso definido por la aplicación

Tipo
Serie

Nombres

Nombre de atributo
Origen_suceso

Nombre de columna
EVTSOURCE

Atributo Tipo de suceso

Descripción
Tipo de suceso: Error(0), Aviso(1), Informativo(2), Auditoría satisfactoria(3), Fallo de auditoría(4), Desconocido(5)

Tipo
Entero

Nombres

Nombre de atributo
Tipo_suceso

Nombre de columna
EVTTYPE

Atributo ID de suceso

Descripción
ID del suceso

Tipo
Entero

Nombres

Nombre de atributo
ID_suceso

Nombre de columna
EVTID

Atributo Categoría de suceso

Descripción
Categoría del suceso

Tipo
Serie

Nombres

Nombre de atributo
Categoría_suceso

Nombre de columna
EVTCATEG

Atributo Mensaje

Descripción
Mensaje del suceso

Tipo
Serie

Nombres

Nombre de atributo
Mensaje

Nombre de columna
MESSAGE

Atributo Hora de generación

Descripción
Hora a la que se generó el suceso

Tipo
Time

Nombres

Nombre de atributo
Hora_generación

Nombre de columna
TIMESTAMP

Resumen de archivos de registro

Los atributos de este grupo de atributos se incluyen en los grupos de atributos de resumen cuando se selecciona esta opción en las propiedades avanzadas del origen de datos.

Se crea un nodo Resumen para cada origen de datos de Archivo de registro cuando se selecciona **Incluir atributo en grupo de atributos de resumen** en las propiedades avanzadas del origen de datos. El nombre del nodo de resumen es el nombre del origen de datos al que se añade Summary al final.

La lista siguiente contiene información sobre cada uno de los atributos predeterminados del grupo de atributos Resumen del archivo de registro. Estos atributos siempre se incluyen en los grupos de atributos de resumen. Si selecciona **Incluir atributo en grupo de atributos de resumen**, consulte el paso "9" en la página 1304 en ("Supervisión de un archivo de registro" en la página 1300), el grupo de atributos de resumen para ese grupo de atributos de registro también contiene cada uno de los atributos seleccionados. Los valores son una copia del atributo correspondiente del grupo de atributos del archivo de registro.

Todos los atributos sumandos constituyen una clave y la tabla de resumen incluyen una fila por cada conjunto exclusivo de claves. La fila indica el número de registros recibidos durante el intervalo donde todas las claves proporcionadas correspondían al valor notificado en los atributos correspondientes.

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se han recopilado los datos.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo Unidad de intervalo

Descripción
Número de segundos entre la generación de atributos de resumen

Tipo
Entero (indicador)

Nombres

Nombre de atributo
_Interval_Unit

Nombre de columna
IU

atributo Intervalo

Descripción
Desplazamiento del intervalo actual dentro de la siguiente unidad mayor de tiempo (por ejemplo, minutos dentro de una hora)

Tipo
Entero (indicador)

Nombres

Nombre de atributo
_Interval

Nombre de columna
INV

Atributo Ocurrencias

Descripción
Número de apariciones registradas durante el intervalo

Tipo
Entero (indicador)

Nombres

Nombre de atributo
_Occurrences

Nombre de columna
OCC

Atributo LocalTimeStamp

Descripción
Hora a la que se han generado los datos de resumen

Tipo
Indicación de fecha y hora

Nombres

Nombre de atributo
_LocalTimeStamp

Nombre de columna
LTS

Atributo DateTime

Descripción
Hora a la que se han generado los datos de resumen

Tipo
Serie

Nombres

Nombre de atributo
_Date_Time

Nombre de columna
DT

Atributo Nombre de la unidad de intervalo

Descripción
Descripción de palabra de la unidad de intervalo

Tipo
Serie

Nombres

Nombre de atributo
_Interval_Unit_Name

Nombre de columna
IUN

Grupo de atributos de registro binario de AIX

El grupo de atributos de registro binario de AIX muestra sucesos del registro binario de AIX tal como lo ha seleccionado la cadena de mandato `errpt`.

La lista siguiente contiene información sobre cada atributo del grupo de atributos de registro binario de AIX:

Nota: Agent Builder impide la eliminación, la reordenación o el cambio del tamaño de los atributos `Identificador`, `ErrptTimestamp`, `Tipo`, `Clase`, `ResourceName` y `Descripción`. El agente analiza los datos que se devuelve de un mandato `errpt` en función de las columnas dentro de la línea de texto. Estas columnas están definidas por el orden y el tamaño de los atributos `Identificador`, `ErrptTimestamp`, `Tipo`, `Clase`, `ResourceName` y `Descripción`. La eliminación, reordenación o cambio del tamaño de estos atributos, cambia el atributo en el que entran las diferentes columnas. La fila resultante tal como aparece en Tivoli Monitoring es, por lo tanto, incorrecta.

Sin embargo, puede renombrar estos atributos.

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Identifier: este atributo es un atributo clave

Descripción
Identificador de suceso informado por `errpt`

Tipo
Serie

Nombres

Nombre de atributo
Identificador

Nombre de columna
IDENTIFICADOR

Atributo ErrptTimestamp

Descripción
Hora a la que se registra el suceso informado por `errpt`.

Nota: Este atributo está oculto durante el tiempo de ejecución. Este atributo contiene un valor sin formato. Otros atributos derivados de este atributo muestran el valor de una forma más útil. Este atributo está disponible desde el Agent Builder para ese fin, pero no es visible de forma predeterminada en el entorno de Tivoli Monitoring durante el tiempo de ejecución. Si desea hacerlo visible, seleccione el atributo en la página **Definición de origen de datos** en el Agent Editor y seleccione **Visualizar atributo en Tivoli Enterprise Portal**.

Tipo
Serie

Nombres

Nombre de atributo
ErrptTimestamp

Nombre de columna
ERRPTTIMES

Tipo

Descripción
Tipo de suceso de un único carácter informado por `errpt`, uno de `I(NFO)`, `P(END/ERF/ERM)`, `T(EMP)` y `U(NKN)`

Tipo
Serie

Nombres

Nombre de atributo
Tipo

Nombre de columna
TYPE

Atributo Clase: este atributo es un atributo clave

Descripción
Clase de suceso informado por `errpt`, uno de `Hardware`, `Software`, `Operador` e `Indeterminado`. Estos valores están enumerados. Los valores sin formato para utilizar con situaciones son H, S, 0 y U.

Tipo
Serie

Nombres

Nombre de atributo
Clase

Nombre de columna
CLASS

ResourceName

Descripción
Nombre de recurso informado por `errpt`, identifica el origen del registro de errores

Tipo
Serie

Nombres

Nombre de atributo
ResourceName

Nombre de columna
RESOURCENA

Atributo Descripción

Descripción
Descripción informada por `errpt`, normalmente un mensaje de texto corto que describe la naturaleza del error

Tipo
Serie

Nombres

Nombre de atributo
Descripción

Nombre de columna
DESCRIPTIO

Atributo LogFile

Descripción
Nombre completo del registro binario de `errpt` incluida la vía de acceso.

Nota: Este atributo está oculto durante el tiempo de ejecución. Este atributo contiene un valor sin formato. Otros atributos derivados de este atributo muestran el valor de una forma más útil. Este atributo está disponible desde el Agent Builder para ese fin, pero no es visible de forma predeterminada en el entorno de Tivoli Monitoring durante el tiempo de ejecución. Si desea hacerlo visible, seleccione el atributo en la página **Definición de origen de datos** en el Agent Editor y seleccione **Visualizar atributo en Tivoli Enterprise Portal**.

Tipo
Serie

Nombres

Nombre de atributo
LogFile

Nombre de columna
LOGFILE

Atributo Sistema

Descripción
Nombre de host del sistema en el que se ha recopilado el error

Tipo
Serie

Nombres

Nombre de atributo
Sistema

Nombre de columna
SYSTEM

Atributo LogName

Descripción
Nombre base del registro binario de `errpt` del que se ha recopilado el registro

Tipo
Serie

Nombres

Nombre de atributo
LogName

Nombre de columna
LOGNAME

Atributo LogPath

Descripción
Nombre de directorio que contiene el registro binario de `errpt` desde el que se ha recopilado el registro

Tipo
Serie

Nombres

Nombre de atributo
LogPath

Nombre de columna
LOGPATH

Atributo EntryTime

Descripción
Hora a la que se ha registrado el suceso según ha informado `errpt` en el formato de indicación de fecha y hora de Tivoli. Esta hora no es necesariamente la misma que la de cuando el agente recibió el suceso, tal como está registrado en el campo **`Indicación de fecha y hora`**.

Tipo
Indicación de fecha y hora

Nombres

Nombre de atributo
EntryTime

Nombre de columna
ENTRYTIME

Grupos de atributos de Supervisión y Notificación

Definiciones de los grupos de atributos Supervisor y Notificación.

Los 4 primeros son específicos de los supervisores y el último corresponde a las notificaciones (todos están relacionados con JMX).

Cada uno se lista con una indicación de si está basado en sucesos o no. Para los grupos de atributos que no están basados en sucesos, los datos se recopilan cuando es necesario. Para los grupos de atributos basados en sucesos, el agente mantiene una memoria caché de los 100 últimos sucesos recibidos. Éstos se utilizan para responder a solicitudes de Tivoli Enterprise Portal. Los sucesos se reenvían inmediatamente para someterlos a análisis mediante situaciones y almacenamiento.

Notificaciones de contador
El grupo de atributos Notificaciones de contador es un grupo de atributos que no está basado en sucesos que envía suceso recibidos por todos los supervisores contadores.

La lista siguiente contiene información sobre todos los atributos del grupo de atributos Notificaciones de contador:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se han recopilado los datos.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo Tipo de notificación

Descripción
Tipo de notificación que se ha recibido. Describe como el atributo observado de MBean ha desencadenado la notificación.

Tipo
Serie

Nombres

Nombre de atributo
Notification_Type

Nombre de columna
NOTIFICATI

Atributo ID de supervisor

Descripción
ID del supervisor que ha generado esta notificación

Tipo
Entero

Nombres

Nombre de atributo
Monitor_ID

Nombre de columna
MONITOR_ID

Atributo MBean observado

Descripción
MBean cuyo atributo se está supervisando

Tipo
Serie

Nombres

Nombre de atributo
Observed_MBean

Nombre de columna
OBSERVED_M

Atributo Atributo observado

Descripción
Nombre del atributo que se supervisa en MBean observado

Tipo
Serie

Nombres

Nombre de atributo
Observed_Attribute

Nombre de columna
OBSERVED_A

Atributo Umbral

Descripción
Umbral actual del supervisor

Tipo
Serie

Nombres

Nombre de atributo
Umbral

Nombre de columna
THRESHOLD

Atributo Desplazamiento

Descripción
Valor añadido al umbral cada vez que el atributo supera el umbral. Este valor genera un nuevo umbral.

Tipo
Serie

Nombres

Nombre de atributo
Desplazamiento

Nombre de columna
OFFSET

Atributo Módulo

Descripción
Valor máximo del atributo. Cuando se alcanza este valor, se vuelve a empezar a contar desde cero.

Tipo
Entero

Nombres

Nombre de atributo
Módulo

Nombre de columna
MODULUS

Atributo Valor de contador

Descripción
Valor del contador que ha desencadenado la notificación

Tipo
Entero

Nombres

Nombre de atributo
Counter_Value

Nombre de columna
COUNTER_VA

Atributo Indicación de fecha y hora de la notificación

Descripción
Hora a la que se desencadenó la notificación

Tipo
Time

Nombres

Nombre de atributo
Notification_Time_Stamp

Nombre de columna
NOTIFICAT0

Atributo Mensaje de notificación

Descripción
Mensaje de la notificación

Tipo
Serie

Nombres

Nombre de atributo
Notification_Message

Nombre de columna
NOTIFICAT1

Notificaciones de medidores
El grupo de atributos Notificaciones de medidores es un grupo de atributos que no está basado en sucesos que envía sucesos recibidos por todos los supervisores medidores.

La lista siguiente contiene información sobre todos los atributos del grupo de atributos Notificaciones de medidores:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se han recopilado los datos.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo Tipo de notificación

Descripción
Tipo de notificación que se ha recibido. Describe como el atributo observado de MBean ha desencadenado la notificación.

Tipo
Serie

Nombres

Nombre de atributo
Notification_Type

Nombre de columna
NOTIFICATI

Atributo ID de supervisor

Descripción
ID del supervisor que ha generado esta notificación

Tipo
Entero

Nombres

Nombre de atributo
Monitor_ID

Nombre de columna
MONITOR_ID

Atributo MBean observado

Descripción
MBean cuyo atributo se está supervisando

Tipo
Serie

Nombres

Nombre de atributo
Observed_MBean

Nombre de columna
OBSERVED_M

Atributo Atributo observado

Descripción
Nombre del atributo que se supervisa en MBean observado

Tipo
Serie

Nombres

Nombre de atributo
Observed_Attribute

Nombre de columna
OBSERVED_A

Atributo Umbral inferior

Descripción
Umbral que el supervisor vigila por si el atributo observado lo cruza

Tipo
Serie

Nombres

Nombre de atributo
Low_Threshold

Nombre de columna
LOW_THRESH

Atributo Umbral superior

Descripción
Umbral que el supervisor vigila por si el atributo observado lo cruza

Tipo
Serie

Nombres

Nombre de atributo
High_Threshold

Nombre de columna
HIGH_THRES

Atributo Valor de medidor

Descripción
Valor del medidor que ha desencadenado la notificación

Tipo
Serie

Nombres

Nombre de atributo
Gauge_Value

Nombre de columna
MODULUSGAUGE_VALU

Atributo Indicación de fecha y hora de la notificación

Descripción
Hora a la que se desencadenó la notificación

Tipo
Time

Nombres

Nombre de atributo
Notification_Time_Stamp

Nombre de columna
NOTIFICAT0

Atributo Mensaje de notificación

Descripción
Mensaje de la notificación

Tipo
Serie

Nombres

Nombre de atributo
Notification_Message

Nombre de columna
NOTIFICAT1

Supervisores registrados
El grupo de atributos Supervisores registrados es un grupo de atributos basado en sucesos que muestra una lista de todos los supervisores de JMX que el agente crea.

La lista siguiente contiene información acerca de todos los atributos que componen el grupo de atributos de Supervisores registrados:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se han recopilado los datos.

Tipo
Time

Nombres

Nombre de atributo
indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo ID de supervisor - Este atributo es un atributo clave

Descripción
Identificador entero exclusivo de un supervisor.

Tipo
Entero

Nombres

Nombre de atributo
Monitor_ID

Nombre de columna
MONITOR_ID

Atributo Parámetros del supervisor

Descripción
Parámetros utilizados para crear el supervisor

Tipo
Serie

Nombres

Nombre de atributo
Monitor_Parameters

Nombre de columna
MONITOR_PA

Atributo Nombre del supervisor

Descripción
Nombre de objeto JMX del MBean del supervisor

Tipo
Serie

Nombres

Nombre de atributo
Monitor_Name

Nombre de columna
MONITOR_NA

Notificaciones de cadena
El grupo de atributos Notificaciones de cadena es un grupo de atributos que no está basado en sucesos que envía suceso recibidos por todos los supervisores de cadenas.

La lista siguiente contiene información sobre todos los atributos del grupo de atributos Notificaciones de cadena:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se han recopilado los datos.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo Tipo de notificación

Descripción
Tipo de notificación que se ha recibido. Describe como el atributo observado de MBean ha desencadenado la notificación.

Tipo
Serie

Nombres

Nombre de atributo
Notification_Type

Nombre de columna
NOTIFICATI

Atributo ID de supervisor - Este atributo es un atributo clave

Descripción
Identificador entero exclusivo de un supervisor.

Tipo
Entero

Nombres

Nombre de atributo
Monitor_ID

Nombre de columna
MONITOR_ID

Atributo MBean observado

Descripción
MBean cuyo atributo se está supervisando

Tipo
Serie

Nombres

Nombre de atributo
Observed_MBean

Nombre de columna
OBSERVED_M

Atributo Atributo observado

Descripción
Nombre del atributo que se supervisa en MBean observado

Tipo
Serie

Nombres

Nombre de atributo
Observed_Attribute

Nombre de columna
OBSERVED_A

Atributo Cadena de comparación

Descripción
Cadena utilizada en la operación de comparación

Tipo
Serie

Nombres

Nombre de atributo
Compare_String

Nombre de columna
COMPARE_ST

Atributo Valor de serie

Descripción
Valor del atributo que ha desencadenado la notificación

Tipo
Serie

Nombres

Nombre de atributo
String_Value

Nombre de columna
STRING_VAL

Atributo Indicación de fecha y hora de la notificación

Descripción
Hora a la que se desencadenó la notificación

Tipo
Time

Nombres

Nombre de atributo
Notification_Time_Stamp

Nombre de columna
NOTIFICAT0

Atributo Mensaje de notificación

Descripción
Mensaje de la notificación

Tipo
Serie

Nombres

Nombre de atributo
Notification_Message

Nombre de columna
NOTIFICAT1

Grupos de atributos de sucesos SNMP

Los grupos de atributos de sucesos SNMP se utilizan para recibir condiciones de excepción e informaciones. Estos grupos de atributos son grupos de atributos basados en sucesos

La siguiente lista contiene información sobre cada atributo de los grupos de atributos de sucesos SNMP:

Nota: Puede cambiar el nombre de visualización predeterminado de estos atributos. Estos nombres de visualización son distintos al ID interno de cada atributo.

Enterprise_OID
El OID de empresa que ha generado la condición de excepción.

Source_Address
Nombre de host o dirección IP del agente SNMP que ha enviado la condición de excepción.

Generic_Trap
Número de condición de excepción genérica extraído de la condición de excepción recibida. Posibles valores:

```
0 ColdStart
1 WarmStart
2 LinkDown
3 LinkUp
4 Authentication Failure
5 EGPNeighborLoss
```

Specific_Trap
Número de condición de excepción específico de la empresa extraído de la condición de excepción recibida. Sólo se aplica cuando Generic_Trap = 6.

Alert_Name
Nombre de condición de excepción según lo especificado en la definición del archivo de configuración de condiciones de excepción.

Category
Categoría de condición de excepción según lo especificado en la definición del archivo de configuración de condiciones de excepción.

Description
Descripción de condición de excepción según lo especificado en la definición del archivo de configuración de condiciones de excepción. La longitud máxima de descripción es 256 caracteres.

Enterprise_Name
Nombre de Enterprise para condición de excepción según lo especificado en el archivo de configuración de condiciones de excepción y determinado a través del identificador de objetos de condiciones de excepción.

Source_Status
Estado del agente que originó la condición de excepción después de enviarla según lo especificado en la definición de condiciones de excepción del archivo de configuración de condiciones de excepción.

Source_Type
Tipo del agente que originó la condición de excepción según lo especificado en la definición de condición de excepción del archivo de configuración de condiciones de excepción.

Event_Variables
Datos de enlace de variables (VarBind) recibidos en la unidad de datos de protocolo (PDU) de condición de excepción. La cadena se construye como:

```
{OID[type]=value}{OID[type]=value}{oid[type]=value}...
```

Donde:

oid
Identificador de objeto de variable MIB

tipo
Tipo de datos SMI

valor
Valor de variable

{}
Cada triplete se encierra entre llaves ({}).

Nota: Los atributos nombre de alerta, Categoría, Descripción, Enterprise_Name, Source_Status y Source_Type proporcionan información adicional. En la ventana **Navegador MIB de SNMP**, marque el recuadro de selección **Incluir atributos que muestran información definida en el archivo de configuración de condición de excepción** para incluir estos atributos.

Grupos de atributos de Sucesos JMX

Los grupos de atributos de sucesos JMX se utilizan para recibir notificaciones de un servidor de MBean.

Estos grupos de atributos son grupos de atributos que no están basados en sucesos y se generan con los siguientes atributos que el desarrollador del agente puede editar.

La lista siguiente contiene información sobre todos los atributos de Grupos de atributos de sucesos JMX:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se han recopilado los datos.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo Tipo

Descripción
Tipo de notificación

Tipo
Serie

Nombres

Nombre de atributo
Tipo

Nombre de columna
TYPE

Atributo Origen

Descripción
MBean que ha provocado el envío de la notificación

Tipo
Serie

Nombres

Nombre de atributo
Origen

Nombre de columna
SOURCE

Atributo Número de secuencia

Descripción
Número de secuencia del objeto de notificación

Tipo
Serie

Nombres

Nombre de atributo
Sequence_Number

Nombre de columna
SEQUENCE_N

Atributo Mensaje

Descripción
Mensaje de notificación

Tipo
Serie

Nombres

Nombre de atributo
Mensaje

Nombre de columna
MESSAGE

Atributo Datos de usuario

Descripción
Objeto de datos de usuario de la notificación

Tipo
Serie

Nombres

Nombre de atributo
User_Data

Nombre de columna
USER_DATA

Grupo de atributos de ping

El grupo de atributos de ping contiene los resultados de pings de ICMP que se envían a listas de dispositivos.

La siguiente lista contiene información sobre cada atributo del grupo de atributos de ping:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora recopilada del sistema de agente cuando se creó la fila de datos y se envió del agente al servidor de Tivoli Enterprise Monitoring. O se ha almacenado con fines históricos. Representa el huso horario local del sistema agente.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributos Dirección: este atributo es un atributo clave

Descripción
Dirección IP del host que se supervisa.

Tipo
Cadena con valor enumerado. El valor UNKNOWN_ADDRESS aparece si la dirección IP es desconocida. El almacén y las consultas devuelven 0.0.0.0 para esta numeración. Los otros valores de dirección IP aparecen tal cual.

Nombres

Nombre de atributo
Dirección

Nombre de columna
PNGADDR

Atributo Entrada de dispositivo: este atributo es un atributo clave

Descripción
Entrada en el archivo de lista de dispositivos para este nodo.

Tipo
Serie

Nombres

Nombre de atributo
Device_Entry

Nombre de columna
PINGDEVC

Atributo Tiempo de respuesta actual

Descripción
Tiempo de respuesta de red actual para las solicitudes ICMP del nodo gestionado en milisegundos.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los números. Los valores definidos son `TIMEOUT(-1)` y `SEND_FAILURE(-2)`. Cualquier otro valor muestra el valor numérico.

Nombres

Nombre de atributo
Current_Response_Time

Nombre de columna
PINGRSTM

Atributo Nombre

Descripción
Nombre de host del nodo gestionado. Si la dirección de nodo no se puede resolver a través de DNS, entonces aparece la dirección IP decimal con puntos.

Tipo
Cadena con valor enumerado. Aparece el valor UNKNOWN_HOSTNAME si el nombre de host es desconocido. El almacén y las consultas devuelven 0.0.0.0 para esta numeración. Cualquier otro valor de nombre de host se visualiza tal cual.

Nombres

Nombre de atributo
Nombre

Nombre de columna
PNGNAME

Atributo Descripción de nodo

Descripción
Descripción del nodo gestionado.

Tipo
Serie

Nombres

Nombre de atributo
Node_Description

Nombre de columna
PNGDESC

Atributo Estatus de nodo

Descripción
Estado operativo actual del nodo gestionado.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los números. Los valores definidos son `INVALID(-2)`, `UNKNOWN(-1)`, `INACTIVE(0)` y `ACTIVE(1)`.

Nombres

Nombre de atributo
Node_Status

Nombre de columna
PNGSTAT

Atributo Tipo de nodo

Descripción
Tipo del nodo gestionado. Si el nodo está en línea, será un nodo IP. Si está fuera de línea, el tipo será desconocido.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los números. Los valores definidos son `UNKNOWN(0)` y `IP NODE(1)`.

Nombres

Nombre de atributo
Node_Type

Nombre de columna
PNGTYPE

Indicación de fecha y hora de estatus

Descripción
Fecha y hora en que el nodo se comprobó por última vez.

Tipo
Time

Nombres

Nombre de atributo
Status_Timestamp

Nombre de columna
PNGTMSP

Grupos de atributos HTTP

Los dos grupos de atributos HTTP, `URL gestionados` y `Objetos de URL`, se utilizan para recibir información de los URL y los objetos contenidos en estos URL.

Para obtener información sobre la sintaxis utilizada en las tablas de URL gestionadas y Objetos URL, consulte (“Campos específicos para atributos HTTP” en la página 1337).

URL gestionados

La siguiente lista contiene información sobre cada atributo del grupo de atributos de URL gestionado:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se han recopilado los datos.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo URL: este atributo es un atributo clave

Descripción
URL que se está supervisando.

Tipo
Serie

Nombres

Nombre de atributo
URL

Nombre de columna
HTTPURL

Atributo de tiempo de respuesta

Descripción
Cantidad de tiempo que ha tardado en descargar la respuesta en milisegundos.

Tipo
Entero con el valor enumerado. La cadena se visualiza en Tivoli Enterprise Portal, el almacén y las consultas devuelven el número. El valor definido es `TIMEOUT (-1)`.

Nombres

Nombre de atributo
Response_Time

Nombre de columna
HTTPURL

Atributo tamaño de página

Descripción
Tamaño de la página devuelta por la solicitud HTTP.

Tipo
Entero con el valor enumerado. La cadena se visualiza en Tivoli Enterprise Portal, el almacén y las consultas devuelven el número. El valor definido es `NO_RESPONSE_RECEIVED(-1)`.

Nombres

Nombre de atributo
Page_Size

Nombre de columna
PAGESZ

Atributo Objetos de página

Descripción
Número total de objetos asociados con la página supervisada.

Tipo
Entero con el valor enumerado. La cadena se visualiza en Tivoli Enterprise Portal, el almacén y las consultas devuelven el número. El valor definido es `NOT_COLLECTED(-1)`.

Nombres

Nombre de atributo
Page_Objects

Nombre de columna
PGOBJS

Atributo Tamaño total de objeto

Descripción
Tamaño de la página devuelta por la solicitud HTTP.

Tipo
Entero con el valor enumerado. La cadena se visualiza en Tivoli Enterprise Portal, el almacén y las consultas devuelven el número. El valor definido es `NOT_COLLECTED(-1)`.

Nombres

Nombre de atributo
Total_Object_Size

Nombre de columna
TOTOSZ

Atributo Título de página

Descripción
Título de la página de la página URL recibida.

Tipo
Serie

Nombres

Nombre de atributo
Page_Title

Nombre de columna
PAGETTL

Atributo Tipo de servidor

Descripción
Tipo de servidor utilizado en el sitio web del URL de destino.

Tipo
Serie

Nombres

Nombre de atributo
Server_Type

Nombre de columna
SRVTYP

Atributo Código de respuesta

Descripción
Código de respuesta de la solicitud HTTP.

Tipo
Entero con el valor enumerado. La cadena se visualiza en Tivoli Enterprise Portal, el almacén y las consultas devuelven el número. El valor definido es `NO_RESPONSE_RECEIVED(-1)`.

Nombres

Nombre de atributo
Response_Code

Nombre de columna
CODE

Atributo Estatus

Descripción
Estatus actual del URL gestionado (Aceptar o descripción de estatus).

Tipo
Serie

Nombres

Nombre de atributo
Estatus

Nombre de columna
STATUS

Atributo Alias de URL

Descripción
Alias especificado por el usuario para el URL.

Tipo
Serie

Nombres

Nombre de atributo
URL_Alias

Nombre de columna
ALIAS

Atributo Datos de usuario

Descripción
Datos de usuario especificados con el URL.

Tipo
Serie

Nombres

Nombre de atributo
User_Data

Nombre de columna
USER

Objetos de URL

La siguiente lista contiene información sobre cada atributo del grupo de atributos Objetos de URL:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se han recopilado los datos.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo URL: este atributo es un atributo clave

Descripción
URL que se está supervisando.

Tipo
Serie

Nombres

Nombre de atributo
URL

Nombre de columna
HTTPURL

Atributo Nombre de objeto

Descripción
Nombre del objeto de página en el URL de destino.

Tipo
Serie

Nombres

Nombre de atributo
Nombre_objeto

Nombre de columna
ONAME

Atributo Tamaño de objeto

Descripción
Tamaño (bytes) del objeto de página en el URL de destino.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los números. Los valores definidos son `NOT_COLLECTED (-1)`, `OBJECT_NOT_FOUND (-2)`. Cualquier otro valor muestra el valor numérico.

Nombres

Nombre de atributo
Object_Size

Nombre de columna
SIZE

Atributo Tiempo de respuesta de objeto

Descripción
Cantidad de tiempo que ha tardado en descargar el objeto en milisegundos.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. El almacén y las consultas devuelven los números. Los valores definidos son `NOT_COLLECTED (-1)`, `NO_RESPONSE_RECEIVED (-2)`, `STATUS_CODE_ERROR (-3)`. Cualquier otro valor muestra el valor numérico.

Nombres

Nombre de atributo
Object_Response_Time

Nombre de columna
ORTIME

Grupos de atributos de Descubrimiento

Un grupo de atributos que representa el conjunto de instancias de subnodo que están definidas para un tipo de subnodo

Al crear un tipo de subnodo, se crea un grupo de atributos que representa el conjunto de instancias de subnodo que están definidas para este tipo de subnodo. Cada uno de estos grupos de atributos incluye el mismo conjunto de atributos.

La lista siguiente contiene información sobre cada atributo de un grupo de atributos de descubrimiento. El nombre del texto en negrita muestra cómo se visualiza el atributo en Tivoli Enterprise Portal:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora del sistema de agente a la que se ha creado la fila de datos y se ha enviado a Tivoli Enterprise Monitoring Server (o se ha almacenado con fines históricos). Representa el huso horario local del sistema agente.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo NSG del subnodo

Descripción
Nombre del sistema gestionado del agente del subnodo.

Tipo
Serie

Nombres

Nombre de atributo
Subnode_MSN

Nombre de columna
SN_MSN

Atributo Afinidad del subnodo

Descripción
Afinidad del agente del subnodo.

Tipo
Serie

Nombres

Nombre de atributo
Subnode_Affinity

Nombre de columna
SN_AFFIN

Atributo Tipo de subnodo

Descripción
El tipo de nodo de este subnodo.

Tipo
Serie

Nombres

Nombre de atributo
Subnode_Type

Nombre de columna
SN_TYPE

Atributo Nombre de recurso de subnodo

Descripción
Nombre de recurso del agente del subnodo.

Tipo
Serie

Nombres

Nombre de atributo
Subnode_Resource_Name

Nombre de columna
SN_RES

Atributo Versión del subnodo

Descripción
La versión del agente del subnodo.

Tipo

Nombres

Nombre de atributo
Subnode_Version

Nombre de columna
SN_VER

Grupo de atributos Estado de actuación

El grupo de atributos Estado de actuación contiene el estado de las acciones que el agente ha procesado.

Este grupo de atributos está basado en sucesos y contiene información sobre cada atributo del grupo de atributos Estatus de actuación:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora que se recopila del agente de sistema, cuando se construyó y se envió la fila de datos desde el agente al servidor de Tivoli Enterprise Monitoring. O se ha almacenado con fines históricos. Representa el huso horario local del sistema agente.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo Nombre de acción

Descripción
El nombre de la acción que se ha ejecutado

Tipo
Serie

Nombres

Nombre de atributo
Action_Name

Nombre de columna
TSKNAME

Atributo Estatus de acción

Descripción
El estado de la acción.

Tipo
Entero con valores enumerados. Los valores son: OK (0), NOT_APPLICABLE (1), GENERAL_ERROR (2), WARNING (3), NOT_RUNNING (4), DEPENDENT_NOT_RUNNING (5), ALREADY_RUNNING (6), PREREQ_NOT_RUNNING (7), TIMED_OUT (8), DOESNT_EXIST (9), UNKNOWN (10), DEPENDENT_STILL_RUNNING (11), INSUFFICIENT_USER_AUTHORITY (12)

Nombres

Nombre de atributo
Action_Status

Nombre de columna
TSKSTAT

Atributo Código de retorno de aplicación de acción

Descripción
El código de retorno de la aplicación que la acción ha iniciado.

Tipo
Entero

Nombres

Nombre de atributo
Action_App_Return_Code

Nombre de columna
TSKAPRC

Atributo Mensaje de acción

Descripción
El mensaje asociado al código de retorno de la acción.

Tipo
Serie

Nombres

Nombre de atributo
Action_Message

Nombre de columna
TSKMSGE

Atributo Instancia de acción

Descripción
La instancia asociada a la salida producida al ejecutar la acción. Si la acción es un mandato del sistema, la instancia será el número de línea de la salida del mandato.

Tipo
Serie

Nombres

Nombre de atributo
Action_Instance

Nombre de columna
TSKINST

Atributo Resultados de acción

Descripción
La salida producida al ejecutar la acción.

Tipo
Serie

Nombres

Nombre de atributo
Action_Results

Nombre de columna
TSKOUTP

Atributo Mandato de acción

Descripción
El mandato ejecutado por la acción.

Tipo
Serie

Nombres

Nombre de atributo
Action_Command

Nombre de columna
TSKCMND

Atributo Nodo de acción

Descripción
El nodo donde se ejecutó la acción.

Tipo
Serie

Nombres

Nombre de atributo
Action_Node

Nombre de columna
TSKORGN

Atributo Subnodo de acción

Descripción
El subnodo donde se ejecutó la acción.

Tipo
Serie

Nombres

Nombre de atributo
Action_Subnode

Nombre de columna
TSKSBND

Atributo ID de acción

Descripción
ID de la acción.

Tipo
Entero

Nombres

Nombre de atributo
Action_ID

Nombre de columna
TSKID

Atributo Tipo de acción

Descripción
Tipo de la acción.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal, el almacén y las consultas devuelven los números. Los valores definidos son: UNKNOWN (0), AUTOMATION (1).

Nombres

Nombre de atributo
Action_Type

Nombre de columna
TSKTYPE

Atributo Propietario de acción

Descripción
Nombre de la situación o el usuario que inició la acción.

Tipo
Serie

Nombres

Nombre de atributo
Action_Owner

Nombre de columna
TSKOWNR

Grupo de atributos Estado del archivo de registro

El grupo de atributos Estado del archivo de registro contiene información que refleja el estatus de los archivos de registro que está supervisando este agente.

El grupo de atributos Estado del archivo de registro se incluye si tiene un grupo de atributos de registro y el agente es la versión mínima predeterminada de Tivoli Monitoring 6.2.1 o posterior. El grupo de atributos Estado del archivo de registro incluye dos atributos definidos como números de 64 bits, por lo que pueden manejar archivos grandes. El soporte de atributos numérico de 64 bits lo proporciona Tivoli Monitoring versión 6.2.1 o posterior.

La lista siguiente contiene información sobre todos los atributos del grupo de atributos Estado del archivo de registro:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
El valor es la hora recopilada del sistema de agente, cuando se ha creado la fila de datos y se ha enviado desde el agente al servidor de Tivoli Enterprise Monitoring. O se ha almacenado con fines históricos. Representa el huso horario local del sistema agente.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo Nombre de tabla: este atributo es clave

Descripción
El nombre de la tabla en la que se supervisa este registro

Tipo
Serie

Nombres

Nombre de atributo
Table_Name

Nombre de columna
TBLNAME

Atributo Nombre de archivo: este atributo es clave

Descripción
El nombre del archivo que se supervisa

Tipo
Serie

Nombres

Nombre de atributo
File_Name

Nombre de columna
FILNAME

Atributo Patrón de RegEx: este atributo es clave

Descripción
El patrón de la expresión regular (si es que existe) que ocasionó que se supervisara este archivo

Tipo
Serie

Nombres

Nombre de atributo
RegEx_Pattern

Nombre de columna
REPATRN

Atributo Tipo de archivo

Descripción
El tipo de este archivo (archivo normal o conducto)

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. Los valores definidos son UNKNOWN(0), REGULAR FILE(1), PIPE(2)

Nombres

Nombre de atributo
File_Type

Nombre de columna
FILTYPE

Atributo Estado del archivo

Descripción
El estado del archivo que se supervisa

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. Los valores definidos son: OK(0), PERMISSION DENIED(1), FILE DOES NOT EXIST(2), INTERRUPTED SYSTEM CALL(4), I/O ERROR(5), NO SUCH DEVICE(6), BAD FILE NUMBER(9), OUT OF MEMORY(12), ACCESS DENIED(13), RESOURCE BUSY(16), NOT A DIRECTORY(20), IS A DIRECTORY(21), INVALID ARGUMENT(22), FILE TABLE OVERFLOW(23), TOO MANY OPEN FILES(24), TEXT FILE BUSY(26), FILE TOO LARGE(27), NO SPACE LEFT ON DEVICE(28), ILLEGAL SEEK ON PIPE(29), READ-ONLY FILE SYSTEM(30), TOO MANY LINKS(31), BROKEN PIPE(32)

Nombres

Nombre de atributo
File_Status

Nombre de columna
FILSTAT

Atributo Número de registros coincidentes

Descripción
El número de registros procesados de este registro que coincidían con uno de los patrones especificados

Tipo
Entero

Nombres

Nombre de atributo
Num_Records_Matched

Nombre de columna
RECMTCH

Atributo Número de registros no coincidentes

Descripción
El número de registros procesados enviados a UnmatchLog; no coincidieron con ningún patrón

Tipo
Entero

Nombres

Nombre de atributo
Num_Records_Not_Matched

Nombre de columna
RECUNMT

Atributo Número de registros procesados

Descripción
El número de registros que se procesan de este registro desde el inicio del agente (incluidos los que no son coincidencias/sucesos)

Tipo
Entero

Nombres

Nombre de atributo
Num_Records_Processed

Nombre de columna
RECPROC

Atributo de la posición de archivo actual

Descripción
La posición actual en bytes en el archivo supervisado. Se procesan los datos hasta esta posición, los datos después de esta posición no se procesan. No aplicable para los conductos.

Tipo
Entero

Nombres

Nombre de atributo
Current_File_Position

Nombre de columna
OFFSET

Atributo Tamaño actual del archivo

Descripción
El tamaño actual del archivo supervisado. No aplicable para los conductos.

Tipo
Entero

Nombres

Nombre de atributo
Current_File_Size

Nombre de columna
FILESIZE

Atributo Hora de la última modificación

Descripción
La hora en la que se grabó por última vez el archivo supervisado. No aplicable para los conductos.

Tipo
Indicación de fecha y hora

Nombres

Nombre de atributo
Last_Modification_Time

Nombre de columna
LASTMOD

Atributo Página de códigos

Descripción
La página de códigos de idioma del archivo supervisado

Tipo
Serie

Nombres

Nombre de atributo
Página de códigos

Nombre de columna
CODEPG

Grupo de atributos Estadísticas de RegEx del archivo de registro

El grupo de atributos Estadísticas de RegEx del archivo de registro contiene información que muestra las estadísticas de las expresiones de búsqueda de la expresión regular del archivo de registro.

Las expresiones regulares se pueden utilizar para filtrar registros o para definir registros. Este grupo de atributos muestra información acerca de los dos tipos. Cuando el atributo Tipo de resultado contiene `INCLUDE` o `EXCLUDE`, el filtro se utiliza para filtrar registros. Si el atributo Tipo de resultado contiene `BEGIN` o `END`, el filtro se utiliza para definir registros. Las medidas de CPU son aproximaciones que se basan en la granularidad de los datos que el sistema operativo expone. Estas medidas pueden dar como resultado valores de `0,00` cuando una expresión regular tarda poco tiempo en evaluarse. Utilice los tiempos de CPU para determinar el coste relativo de las expresiones regulares y para optimizar el comportamiento de expresiones regulares específicas.

El grupo de atributos Estadísticas de RegEx del archivo de registro se incluye si tiene un grupo de atributos de registro y el agente es la versión de Tivoli Monitoring 6.2.1 o posterior. La versión mínima de Tivoli Monitoring se selecciona en la página **Información de agente**. Para obtener más información, consulte (“Denominación y configuración del agente” en la página 1205). El grupo de atributos Estadísticas de RegEx del archivo de registro incluye atributos que se definen como números de 64 bits, por lo que pueden manejar largas duraciones. El soporte de atributos numéricos de 64 bits lo proporciona Tivoli Monitoring versión 6.2.1 o posterior.

La lista siguiente contiene información sobre todos los atributos del grupo de atributos Estadísticas de RegEx del archivo de registro:

Atributo Nodo: este atributo es un atributo clave

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Nombres

Nombre de atributo
Nodo

Nombre de columna
ORIGINNODE

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Time

Nombres

Nombre de atributo
Indicación de fecha y hora

Nombre de columna
TIMESTAMP

Atributo Nombre de tabla: este atributo es clave

Descripción
Nombre del grupo de atributos del archivo de registro.

Tipo
Serie

Nombres

Nombre de atributo
Table_Name

Nombre de columna
TBLNAME

Atributo Nombre de atributo: este atributo es clave

Descripción
Nombre del atributo al que se aplica este filtro.

Tipo
Serie

Nombres

Nombre de atributo
Attribute_Name

Nombre de columna
ATRNAME

Número de filtro

Descripción
El número de secuencia, empezando por cero, del filtro que se utiliza para el atributo.

Tipo
Entero (propiedad numérica)

Nombres

Nombre de atributo
Filter_Number

Nombre de columna
FLTRNUM

Atributo Tipo de resultado

Descripción
El tipo de resultado puede ser INCLUDE o EXCLUDE para aceptar o rechazar el atributo si el filtro coincide. El tipo de resultado puede ser BEGIN o END para especificar el principio o el final de un registro para registros de varias líneas.

Tipo
Entero con valores enumerados. Las cadenas se visualizan en Tivoli Enterprise Portal. Si el filtro se utiliza para filtrar registros, los valores definidos son `INCLUDE(1)` o `EXCLUDE(2)`. Si el filtro se utiliza para definir registros, los valores definidos son `BEGIN(3)` o `END(4)`.

Nombres

Nombre de atributo
Result_Type

Nombre de columna
RSTTYPE

Atributo Tiempo promedio de procesador

Descripción
El tiempo medio (en segundos) del procesador utilizado para procesar el filtro para este atributo. El tiempo promedio de procesador son los segundos totales de procesador divididos entre el número de filtros.

Tipo
Entero (Medidor)

Nombres

Nombre de atributo
Average_Processor_Time

Nombre de columna
CPUTAVG

Atributo Tiempo de procesador

Descripción
El tiempo total (en segundos) del procesador utilizado para procesar el filtro para este atributo. El tiempo de procesador es acumulativo y se trunca, no se redondea. Es similar al archivo `/proc/<pid>/task/`*`thread`*`/stat` de Linux.

Tipo
Entero (Contador)

Nombres

Nombre de atributo
Processor_Time

Nombre de columna
CPUTIME

Atributo Tiempo de procesador máximo

Descripción
Tiempo máximo (en segundos) de procesador utilizado para un único proceso del filtro. Es posible que el máximo sea cero si el filtro no se ha utilizado nunca o si cada proceso del filtro ha tardado menos de 0,01 segundos.

Tipo
Entero (Medidor)

Nombres

Nombre de atributo
Max_Processor_Time

Nombre de columna
CPUTMAX

Atributo Tiempo de procesador mínimo

Descripción
Tiempo mínimo (en segundos) de procesador utilizado para un único proceso del filtro. Es posible que el mínimo sea cero si el proceso de un filtro ha tardado menos de 0,01 segundos.

Tipo
Entero (Medidor)

Nombres

Nombre de atributo
Min_Processor_Time

Nombre de columna
CPUTMIN

Atributo Recuento de filtro

Descripción
El número de veces que el filtro se ha ejecutado. Se utiliza con el tiempo de procesador total para computar el tiempo de procesador medio.

Tipo
Entero (Contador)

Nombres

Nombre de atributo
Filter_Count

Nombre de columna
COUNT

Atributo Recuento de filtro coincidente

Descripción
El número de veces que el filtro se ha ejecutado y el atributo ha coincidido.

Tipo
Entero (Contador)

Nombres

Nombre de atributo
Filter_Count_Matched

Nombre de columna
COUNTMA

Atributo Recuento de filtro no coincidente

Descripción
El número de veces que el filtro se ha ejecutado y el atributo no ha coincidido.

Tipo
Entero (Contador)

Nombres

Nombre de atributo
Filter_Count_Unmatched

Nombre de columna
COUNTUN

Atributo Patrón de RegEx: este atributo es clave

Descripción
La expresión regular que se utiliza para la coincidencia.

Tipo
Serie

Nombres

Nombre de atributo
RegEx_Pattern

Nombre de columna
REGXPAT

Atributo Hora de última coincidencia

Descripción
Última vez que se utilizó el filtro y se encontró una coincidencia del resultado.

Tipo
Time

Nombres

Nombre de atributo
Last_Matched_Time

Nombre de columna
LASTMAT

Atributo Hora de última falta de coincidencia

Descripción
Última vez que se utilizó el filtro y no se encontró una coincidencia del resultado.

Tipo
Time

Nombres

Nombre de atributo
Last_Unmatched_Time

Nombre de columna
LASTUMA

Creación de extensiones de soporte de aplicaciones para agentes existentes

Para el entorno IBM Tivoli Monitoring, puede crear un paquete instalable para distribuir espacios de trabajo, situaciones, consultas y mandatos de actuación personalizados que haya creado, como extensión de soporte de aplicaciones para un agente existente.

Antes de empezar

Para obtener más información sobre cómo crear situaciones, espacios de trabajo, mandatos de actuación y consultas personalizados, consulte "Creación de espacios de trabajo, mandatos de Actuación y situaciones" en la página 1408.

Acerca de esta tarea

Importante: Esta tarea no es el modo de añadir soporte de aplicaciones a un agente que se está creando. Para añadir soporte de aplicaciones a un agente que está creando, consulte "Importación de archivos de soporte de aplicaciones" en la página 1444.

Procedimiento

1. En Agent Builder, seleccione **Archivo** > **Nuevo** > **Otro**.
2. Seleccione **Ampliación del soporte de aplicación de Agent Builder** en **Agent Builder**.

3. Pulse **Siguiente** para ir a la página de bienvenida para el asistente **IBM Tivoli Monitoring Application Support**.
4. Pulse **Siguiente** en la página de bienvenida.
5. Entre un nombre para el proyecto y pulse **Finalizar**

Creación de un proyecto de Application Support Extension

Cree un proyecto de Application Support Extension utilizando Agent Builder.

Procedimiento

1. En Agent Builder, seleccione **Archivo** > **Nuevo** > **Otro**.
2. Seleccione **Ampliación del soporte de aplicación de Agent Builder** en **Agent Builder**.
3. Pulse **Siguiente** para ir a la página de bienvenida para el **Asistente de IBM Tivoli Monitoring Application Support Extension**.
4. Pulse **Siguiente** en la página de bienvenida.
5. Entre un nombre para el proyecto y pulse **Finalizar**

Adición de archivos de soporta a un proyecto

Añada los archivos de soporte a un proyecto de Application Support Extension

Antes de empezar

Cree un proyecto de Application Support Extension. Para obtener más información, consulte "Creación de un proyecto de Application Support Extension" en la página 1513.

Procedimiento

1. Pulse con el botón derecho del ratón el proyecto Application Support Extension y seleccione **IBM Tivoli** > **Importar Application Support Extensions**
2. En la ventana **Importar información**, seleccione el nombre del host en el que Tivoli Enterprise Portal Server está ubicado o pulse **Añadir** para añadir uno.
3. En el campo **Aplicación**, especifique el código de producto del agente.
4. Especifique la afinidad del agente para el que está creando el soporte de la aplicación personalizado.

   La afinidad del agente es un identificador interno de Tivoli Monitoring que asocia espacios de trabajo, consultas y otros elementos con el agente. Debe ser exclusivo en la instalación de Tivoli Monitoring. Pulse **Examinar** para abrir la ventana **Tipos de nodo** y seleccionar esta información en la lista en lugar de escribirla.
5. Cuando esté satisfecho con la información de importación, pulse **Finalizar**.
6. En la ventana **Situaciones**, seleccione las situaciones que desea importar desde la lista Situaciones disponibles.

   Pulse **<<** para añadirlas a la lista Situaciones seleccionadas y pulse **Aceptar**. Se creará una carpeta nueva bajo el proyecto que contiene los archivos necesarios para instalar los espacios de trabajo, las situaciones y las consultas.
7. En la ventana **Consultas**, seleccione las consultas que desee importar desde la lista Consultas disponibles.

   Pulse **<<** para añadirlas a la lista Consultas seleccionadas y pulse **Aceptar**.
8. En la ventana **Actuaciones**, elija los mandatos de actuación que desea importar desde la lista Actuaciones disponibles.

   Pulse **<<** para añadirlas a la lista Actuaciones seleccionadas y pulse **Aceptar**. Los archivos de soporte para el agente se colocan en el proyecto en su carpeta adecuada.

Qué hacer a continuación

Puede repetir este proceso para tantos agentes distintos como desee. Agent Builder crea una única imagen de instalación a partir de todos los archivos de soporte del proyecto de Application Support Extension.

Generación de la imagen de instalación de Application Support Extension

Genere una imagen de instalación de Application Support Extension.

Procedimiento

1. Pulse con el botón derecho del ratón sobre el proyecto Application Support Extension y seleccione **IBM Tivoli** > **Crear imagen de instalación de Application Support Extension**.
2. En la ventana **Información de Application Support Extension**, especifique el directorio en el que se debe colocar la imagen.
3. Su Application Support Extension debe tener su propio código de producto. Especifique el código de producto registrado para el nuevo agente. Puede utilizar uno de los códigos de producto reservados para utilizarlos con Agent Builder. Los valores permitidos son `K00-K99`, `K{0-2}{A-Z}` y `K{4-9}{A-Z}`.

   Nota: Estos valores sólo son para uso interno y no están destinados a agentes que se vayan a compartir o vender. Si está creando un agente para compartirlo con otras personas, deberá enviar una nota a toolkit@us.ibm.com para reservar un código de producto. La solicitud de un código de producto debe incluir una descripción del agente que se va a crear. A continuación se asigna, registra y se le devuelve un código de producto. Cuando recibe el código de tres dígitos del producto, se le indica cómo habilitar Agent Builder para utilizar el código de producto asignado.
4. Especifique el nombre de Application Support Extension.
5. Especifique una descripción de Application Support Extension.
6. Entre una versión para Application Support Extension con el formato VVRRMMFF, donde `vv` = número de versión; `rr` = número de release; `mm` = número de modificación (número de fixpack) y `ff` = número de arreglo temporal.
7. Pulse **Finalizar**.

Instalación de Application Support Extension

Instale Application Support Extension

Procedimiento

1. Transfiera la imagen al servidor de Tivoli Enterprise Monitoring y a los servidores del servidor de Tivoli Enterprise Portal.
2. Para instalar el soporte del servidor de Tivoli Enterprise Monitoring, ejecute uno de los mandatos siguientes:
   - En Windows: `install`*`KXX`*`TEMSSupport.bat`
   - En UNIX: `install`*`KXX`*`TEMSSupport.sh`

   El formato para el mandato es el siguiente:

   ```
   installKXXTEMSSupport[.bat | .sh] <dir. instalación ITM> [-s tems_host]
    [-u tems_user]  \[-p tems_password]
   ```
3. Para instalar el soporte del servidor de Tivoli Enterprise Portal, ejecute uno de los mandatos siguientes:
   - En Windows: `install`*`KXX`*`TEPSSupport.bat`
   - En UNIX: `install`*`KXX`*`TEPSSupport.sh`

   El formato para el mandato es el siguiente:

```
installKXXTEPSSupport[.bat | .sh] <Directorio de instalación de ITM> [-r]
```

donde `-r` indica que el servidor de Tivoli Enterprise Portal se debe reiniciar después de la instalación

Conversión de un Proyecto de instalación de soluciones en un proyecto de Application Support Extension

Convierta un **Proyecto de instalación de soluciones** a un proyecto de Application Support Extension

Acerca de esta tarea

Si tiene un **Proyecto de instalación de soluciones** existente que desea convertir en proyecto de Application Support Extension, complete los pasos siguientes:

Nota: En el **Proyecto de instalación de soluciones** solo se migran los archivos de soporte.

Procedimiento

1. Pulse con el botón derecho en el **Proyecto de instalación de soluciones** y seleccione **IBM Tivoli** > **Convertir proyecto de instalación de soluciones**.
2. Escriba el nombre de un nuevo proyecto de Application Support Extension o seleccione uno existente en la lista
3. Pulse **Finalizar**.

Generación del modelo de datos de Cognos

Agent Builder puede generar el modelo de datos de Cognos para cada agente. Utilice el modelo de datos para importar información de agente al Cognos Framework Manager para la creación de informes.

Este modelo de datos de Cognos se puede abrir y ver en Framework Manager, que crea un paquete de modelo para publicarlo en Tivoli Common Reporting. El modelo de datos también se puede personalizar o modificar en Framework Manager antes de la publicación.

Al crear un informe, Agent Builder también permite importar un paquete de informe final al proyecto de Agent Builder. Esta característica permite generar proyectos de agente futuros con los informes que ya forman parte del paquete de agente. Los informes que se empaquetan como parte de la imagen de instalación del agente se pueden importar a Tivoli Common Reporting en el entorno de producción.

Nota: En esta documentación, tenga en cuenta la siguiente convención:

- K*xx* o k*xx* hace referencia al código de producto correspondiente al agente, por ejemplo, k99.
- *Tipo_bd* hace referencia a la base de datos que Tivoli Data Warehouse utiliza, por ejemplo, DB2.

Requisitos previos para generar un modelo de datos de Cognos

Complete estas tareas antes de generar un modelo de datos de Cognos

Acerca de esta tarea

Nota:

- Estos pasos se deben completar solo una vez, ya que todos los modelos de datos futuros generados con Agent Builder utilizarán este entorno.
- Se recomienda crear un entorno de desarrollo aislado para la prueba del agente y la creación de informes.

Procedimiento

1. Instale y configure “Tivoli Data Warehouse” en la página 1516.
2. Crear tablas y procedimientos en Tivoli Data Warehouse.

a) “Creación de tablas y procedimientos en Tivoli Data Warehouse” en la página 1516.

b) “Llenado de Tivoli Data Warehouse con Tivoli Reporting and Analytics Model” en la página 1518.

3. Instale y configure “Tivoli Common Reporting” en la página 1519.
4. Instale y configure “Framework Manager” en la página 1519.

Tivoli Data Warehouse
Acerca de Tivoli Data Warehouse.

Para crear informes, necesita instalar y configurar en su entorno Tivoli Data Warehouse, un Agente de proxy de Warehouse y un Agente de resumen y poda. Para obtener más información, consulte la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Creación de tablas y procedimientos en Tivoli Data Warehouse
Cree o altere la tabla `ManagedSystem` y el procedimiento almacenado en Tivoli Data Warehouse

Acerca de esta tarea

El modelo de datos de Cognos generado incluye una tabla `ManagedSystem` que se utiliza para definir una dimensión `ManagedSystem`. La dimensión `ManagedSystem` permite crear informes que se puedan correlacionar con sistemas gestionados. Por ejemplo, si el agente es un agente de subnodo, la dimensión se puede utilizar para determinar los subnodos que existen para una instancia de agente específica.

La tabla `ManagedSystem` no la crea Tivoli Data Warehouse. Por lo tanto, cuando se genera el agente en Agent Builder, se generan los scripts de SQL para cada plataforma de base de datos, para:

- Crear la tabla `ManagedSystem`. Utilice este script si la tabla no existe en Tivoli Data Warehouse.
- Editar la tabla `ManagedSystem`. Utilice este script si la tabla existe en Tivoli Data Warehouse. Otros productos de informes pueden crear la tabla `ManagedSystem`, pero no lo hacen con todas las columnas necesarias.
- Crear un procedimiento almacenado que llena la tabla `ManagedSystem` a partir de las tablas de Tivoli Data Warehouse.

Ejecute estos scripts solo una vez.

Ejecutar Scripts de DB2 para crear tablas y procedimientos en Tivoli Data Warehouse
Para una base de datos de DB2, utilice estos scripts para crear tablas en Tivoli Data Warehouse

Antes de empezar

Los scripts para DB2 están en el directorio siguiente:

```
reports/db2/Kxx/reports/cognos_reports/itmkxx/db_scripts
```

Procedimiento

1. Todos los scripts generados (`create_table.sql`, `alter_table.sql` y `create_procedure.sql`) usan *`itmuser`* como ID de usuario de Tivoli Data Warehouse. Si *`itmuser`* no es el ID de usuario de Tivoli Data Warehouse en el entorno, cambie todas las apariciones de *`itmuser`* por el ID de usuario correcto.
2. Conecte a Tivoli Data Warehouse como usuario de Tivoli Data Warehouse:

   ```
   db2 connect to <nombre de alias de Tivoli Data Warehouse> user
   <ID de usuario de Tivoli Data Warehouse> using <contraseña>
   ```

3. Determine si la tabla ManagedSystem existe:

   ```
   db2 "select count(*) from sysibm.systables where name = 'MANAGEDSYSTEM'
   and creator=upper ('<ID de usuario de Tivoli Data Warehouse>')"
   ```

4. Cree o altere la tabla.

- Si la consulta devuelve 1, la tabla existe. Ejecute el script alter siguiente:

```
db2 -tvf alter_table.sql
```

- Si la consulta devuelve 0, la tabla no existe. Ejecute el script create:

```
db2 -tvf create_table.sql
```

5. Ejecute el script para crear el procedimiento almacenado:

```
db2 -td@ -f create_procedure.sql
```

Ejecución de scripts de Oracle para crear tablas y procedimientos en Tivoli Data Warehouse
Para una base de datos de Oracle, utilice estos scripts para crear tablas en Tivoli Data Warehouse

Antes de empezar

Los scripts para Oracle están en el directorio siguiente:

```
reports/oracle/K<xx>/reports/cognos_reports/itmk<xx>/db_scripts
```

Procedimiento

1. Todos los scripts generados (`create_table.sql`, `alter_table.sql` y `create_procedure.sql`) usan *`itmuser`* como ID de usuario de Tivoli Data Warehouse. Si *`itmuser`* no es el ID de usuario de Tivoli Data Warehouse en el entorno, cambie todas las apariciones de *`itmuser`* por el ID de usuario correcto.
2. Inicie `sqlplus`:

```
sqlplus <ID de usuario de IBM Tivoli Monitoring>/<contraseña>@
<SID de Tivoli Data Warehouse>
```

3. Determine si la tabla ManagedSystem existe:

```
select count(*) from user_tables where table_name = 'MANAGEDSYSTEM';
```

4. Cree o altere la tabla.
   - Si la consulta devuelve 1, la tabla existe. Ejecute el script alter siguiente:

```
@<vía de acceso a alter_table.sql>;
```

   - Si la consulta devuelve 0, la tabla no existe. Ejecute el script create:

```
@<vía de acceso a create_table.sql>;
```

5. Ejecute el script para crear el procedimiento almacenado:

```
@<vía de acceso a create_procedure.sql>;
```

Ejecución de scripts de SQL Server 2005 y 2008 para crear tablas y procedimientos en Tivoli Data Warehouse

Antes de empezar

Los scripts para SQL Server están en el directorio siguiente:

```
reports/mssql/K<xx>/reports/cognos_reports/itmk<xx>/db_scripts
```

Procedimiento

1. Todos los scripts generados (`create_table.sql`, `alter_table.sql` y `create_procedure.sql`) usan *`itmuser`* como ID de usuario de Tivoli Data Warehouse. Si *`itmuser`* no es el ID de usuario de

Tivoli Data Warehouse en el entorno, cambie todas las apariciones de *itmuser* por el ID de usuario correcto.

2. Determine si existe la tabla ManagedSystem:

```
osql -S <Servidor> -U <ID de usuario de
Tivoli Data Warehouse> -P <contraseña> -d
<nombre de base de datos de Tivoli Data Warehouse> -Q "Select count(*)
from INFORMATION_SCHEMA.TABLES where table_name = 'ManagedSystem'"
```

3. Cree o altere la tabla.
   - Si la consulta devuelve 1, la tabla existe. Ejecute el script alter siguiente:

```
osql -S <Servidor> -U <ID de usuario de Tivoli Data Warehouse> -P
<contraseña> -d
<nombre de base de datos de Tivoli Data Warehouse> -I -n -i <vía de acceso a
alter_table.sql>
```

   - Si la consulta devuelve 0, la tabla no existe. Ejecute el script create:

```
osql -S <Servidor> -U
<ID de usuario de Tivoli Data Warehouse> -P <contraseña> -d
<nombre de base de datos de Tivoli Data Warehouse> -I -n -i <vía de acceso a
create_table.sql>
```

4. Ejecute el script para crear el procedimiento almacenado:

```
osql -S <Servidor> -U <ID
de usuario de Tivoli Data Warehouse> -P
<contraseña> -d <nombre de base de datos de Tivoli Data Warehouse>
-I -n -i <vía de acceso a create_procedure.sql>
```

Llenado de Tivoli Data Warehouse con Tivoli Reporting and Analytics Model

Utilice los scripts de base de datos para llenar el Tivoli Data Warehouse

Acerca de esta tarea

Tivoli Reporting and Analytics Model (TRAM) contiene la base de conocimiento que es común a todos los paquetes de informe. TRAM se instala mediante un conjunto de scripts exclusivos para cada base de datos. Los scripts necesarios para rellenar cada base de datos soportada se incluyen en la imagen de instalación del agente, dentro del directorio reports. Utilice el siguiente procedimiento para crear dimensiones comunes de Tivoli Reporting and Analytics Model en Tivoli Data Warehouse.

Procedimiento

1. Examinar en los scripts de base de datos de Tivoli Reporting y Analytics Model.
2. Extraiga el paquete del agente.
   - En los sistemas Windows, el paquete del agente es k*xx*.zip.
   - En los sistemas Linux y UNIX, el paquete del agente es k*xx*.tgz.
3. Vaya a los scripts de base de datos apropiados.
   - Los scripts de DB2 se encuentran en el paquete del agente en:

```
reports/db2/K<xx>/reports/cognos_reports/itmk<xx>/db_scripts
```

   - Scripts de Oracle se encuentran en el paquete del agente en:

```
reports/oracle/K<xx>/reports/cognos_reports/itmk<xx>/db_scripts
```

   - Los scripts de Microsoft SQL Server se encuentran en el paquete del agente en:

```
reports/mssql/K<xx>/reports/cognos_reports/itmk<xx>/db_scripts
```

4. Ejecute los scripts de la base de datos para generar las dimensiones comunes dentro de Tivoli Data Warehouse. Cada conjunto de scripts proporciona un archivo léame con las instrucciones de uso.

5. Verifique que los scripts han añadido las tablas siguientes a Tivoli Data Warehouse:

```
"Computer System", WEEKDAY_LOOKUP, MONTH_LOOKUP, TIMEZONE_DIMENSION, TIME_DIMENSION
```

Tivoli Common Reporting
Tivoli Common Reporting contiene el motor de Cognos Business Intelligence, que contiene elementos para ayudar con la creación de informes de agente.

Tivoli Common Reporting debe instalarse y configurarse con un origen de datos que se conecte a Tivoli Data Warehouse.

Instalación de Tivoli Common Reporting

Debe instalar Tivoli Common Reporting. Están soportadas las versiones 1.3, 2.1, 2.1.1 o posteriores. Para obtener información acerca de la instalación de Tivoli Common Reporting, consulte Instalación de Tivoli Common Reporting.

Configuración de Tivoli Common Reporting

Debe configurar Tivoli Common Reporting. Para obtener información acerca de la configuración de Tivoli Common Reporting, consulte Configuración de IBM Tivoli Common Reporting.

Crear un origen de datos entre Tivoli Data Warehouse y Tivoli Common Reporting. Para obtener más información, consulte Configuración de la conexión de base de datos. Pulse el tipo de base de datos apropiado. Tenga en cuenta el nombre que se le da al origen de datos. El valor predeterminado es **TDW**.

Nota: El nombre del origen de datos debe coincidir con el nombre en el campo **Origen de datos** de la página **Información de Cognos**. Para obtener más información acerca de la página **Información de Cognos**, consulte “Información de Cognos” en la página 1224.

Framework Manager
Framework Manager es una aplicación incluida con la aplicación Tivoli Common Reporting, pero debe instalarse y configurarse por separado.

Framework Manager se utiliza para ver y modificar modelos de datos y para publicar modelos de datos en Tivoli Common Reporting

Instalación de Framework Manager

Debe instalar Framework Manager. Están soportadas las versiones 8.4, 8.4.1 o posteriores.

Framework Manager se incluye con Tivoli Common Reporting, pero debe instalarse manualmente. Tivoli Common Reporting 1.3 se suministra con Framework Manager 8.4. Tivoli Common Reporting 2.1 y 2.1.1 se incluyen con Framework Manager 8.4.1. Para obtener información sobre la configuración de Framework Manager, consulte Instalación de Framework Manager en *Tivoli Common Reporting: Guía del usuario*.

Configuración de Framework Manager

Debe configurar Framework Manager. Para obtener información sobre la configuración de Framework Manager, consulte Configuración de Framework Manager en *Tivoli Common Reporting: Guía del usuario*.

Creación de informes

Utilice Framework Manager para publicar el modelo de agente y Report Studio para comenzar a crear informes.

Antes de empezar

Cuando se complete el agente, debe instalarse en el entorno de Tivoli Monitoring. Además, la recopilación histórica para el agente debe estar configurada y al agente debe ejecutarse durante al menos un intervalo de carga de almacén. Debe configurarse el resumen y las opciones de configuración del resumen

realizadas en Tivoli Monitoring deben ser idénticas a las opciones de resumen realizadas en Agent Builder. El agente de resumen y poda debe ejecutarse al menos una vez después de que se carguen los datos del agente en el almacén.

1. Instalar, configurar e iniciar el agente.
2. Cree y distribuya al agente una recopilación histórica para cada grupo de atributos para el que desee crear un informe.

   Nota: El intervalo de carga de almacén tiene el valor predeterminado de diario. Sin embargo, puede que desee acortar este intervalo.

   Para obtener más información sobre la recopilación histórica de configuración, consulte Gestión de datos históricos en la *IBM Tivoli Monitoring: Guía del administrador*.
3. En Tivoli Monitoring, configure el resumen para todos los grupos de atributos para los que ha creado recopilaciones históricas en el Paso 2.

   Nota: Cuando configure la recopilación y el resumen históricos, debe esperar el tiempo suficiente para que los datos acaben en las tablas de resumen.

   Nota: De forma predeterminada, el agente de resumen y poda está configurado para ejecutarse una vez al día a las 2 a.m. Puede cambiar este valor. Por ejemplo, puede configurarlo para que se ejecute cada hora. Para obtener más información acerca de la configuración de Tivoli Data Warehouse, consulte Configuración del almacén de datos en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Acerca de esta tarea

La generación de un agente en Agent Builder crea todo un proyecto de Framework Manager, que incluye el modelo de datos y el archivo de proyecto de Framework Manager. Framework Manager puede abrir el archivo de proyecto directamente, lo que abre el modelo de datos para su modificación, personalización o publicación.

Procedimiento

Nota: El modelo de datos generado para el agente contiene todas las dimensiones de tiempo de resumen para cada grupo de atributos: cada hora, a diario, semanal, mensual, trimestral y anual. Las dimensiones solo existen en Tivoli Data Warehouse para el agente si se configura el resumen y poda para el agente. Y además, si se seleccionaron las dimensiones y si el agente de Resumen y Poda creó y llenó las tablas. Se pueden definir y publicar informes en Tivoli Common Reporting que utilicen dimensiones que no existen. Estos informes no funcionan hasta que el agente de resumen y poda crea las tablas de resumen.

1. Abra el Modelo de datos de agente en Framework Manager:
   a) Abra Framework Manager.
   b) En la página de **bienvenida**, pulse **Abrir un proyecto**.

      Consejo: Si está en Framework Manager, pulse **Abrir** en el menú **Archivo**.
   c) Vaya al modelo de datos del agente.
      - Para DB2:

        ```
        reports/db2/Kxx/model/
        ```

      - Para Oracle:

        ```
        reports/oracle/Kxx/model/
        ```

      - Para Microsoft SQL Server:

        ```
        reports/mssql/Kxx/model/
        ```

   d) Seleccione al archivo de proyecto del agente, K*xx*`.cpf`.

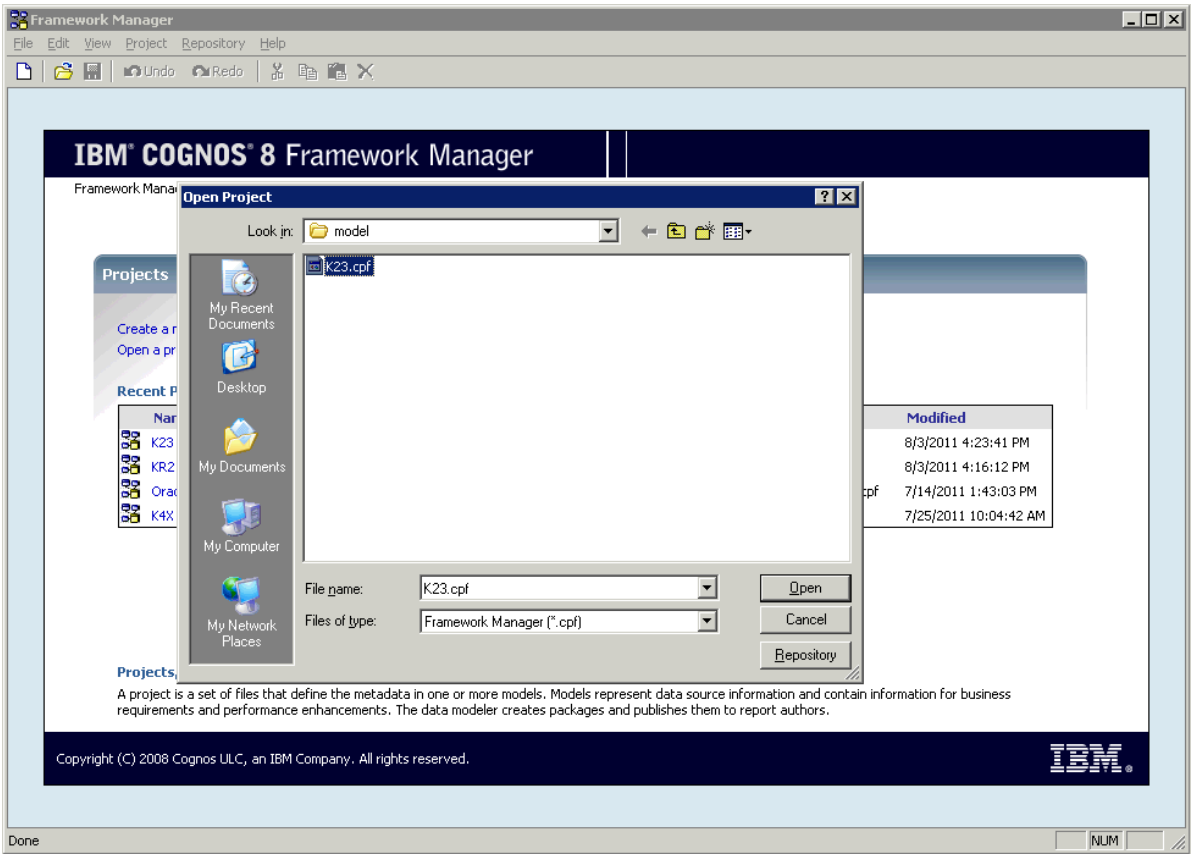


Figura 80. Selección del archivo de proyectos del agente

Nota: Cuando un proyecto de agente se abre en Framework Manager, el nombre de agente se lista bajo Proyectos recientes.

2. Llene la tabla de sistemas gestionados. Para obtener más información, consulte "Llenado de la tabla ManagedSystem" en la página 1525
3. Utilice Framework Manager para publicar el modelo de agente en Tivoli Common Reporting
   a) Abra Framework Manager.
   b) Abra el proyecto del agente.
   c) Expanda **Paquetes** en el árbol de navegación.
   d) Pulse con el botón derecho del ratón en el paquete del agente y seleccione **Publish Packages**.

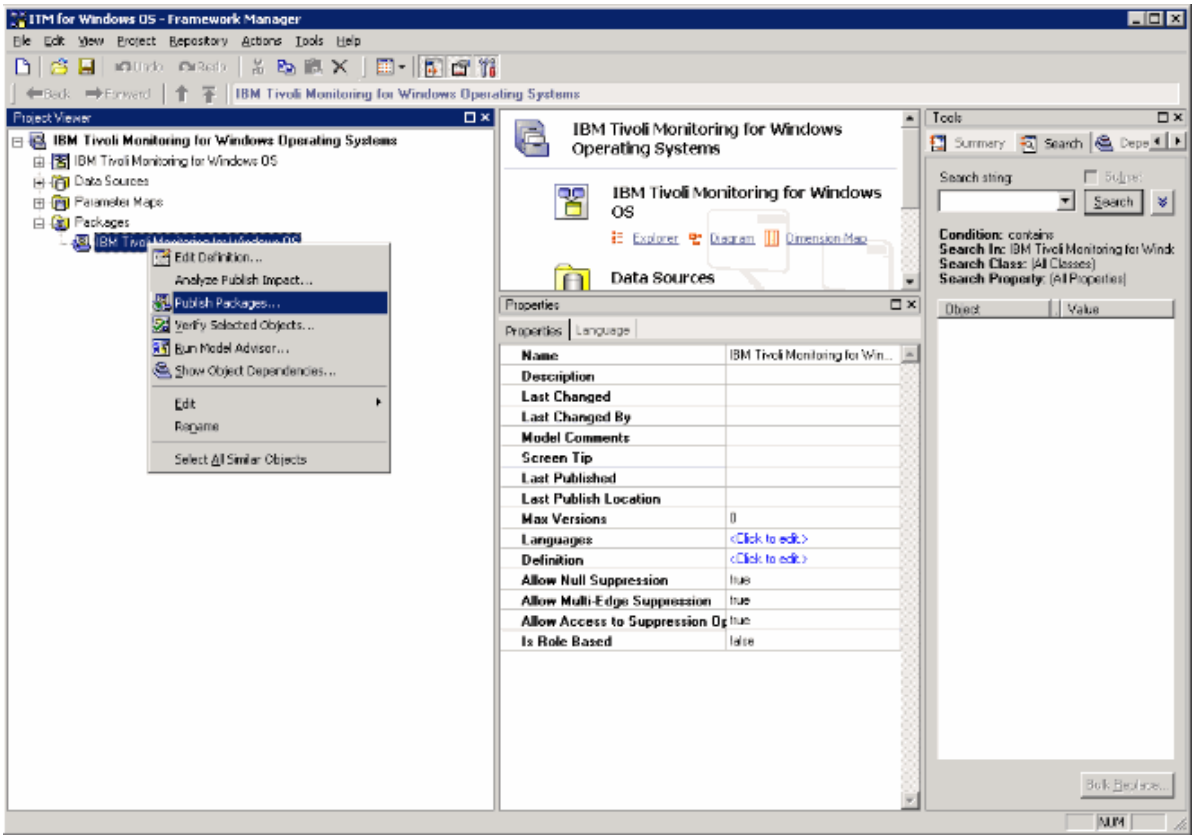


Figura 81. Selección de Publish Packages

4. Utilice Report Studio para crear nuevos informes o plantillas.
   a) Inicie sesión en Tivoli Common Reporting.
   b) Vaya a Carpetas públicas, expanda **Reporting** en el panel de navegación, y seleccione **Common Reporting**.

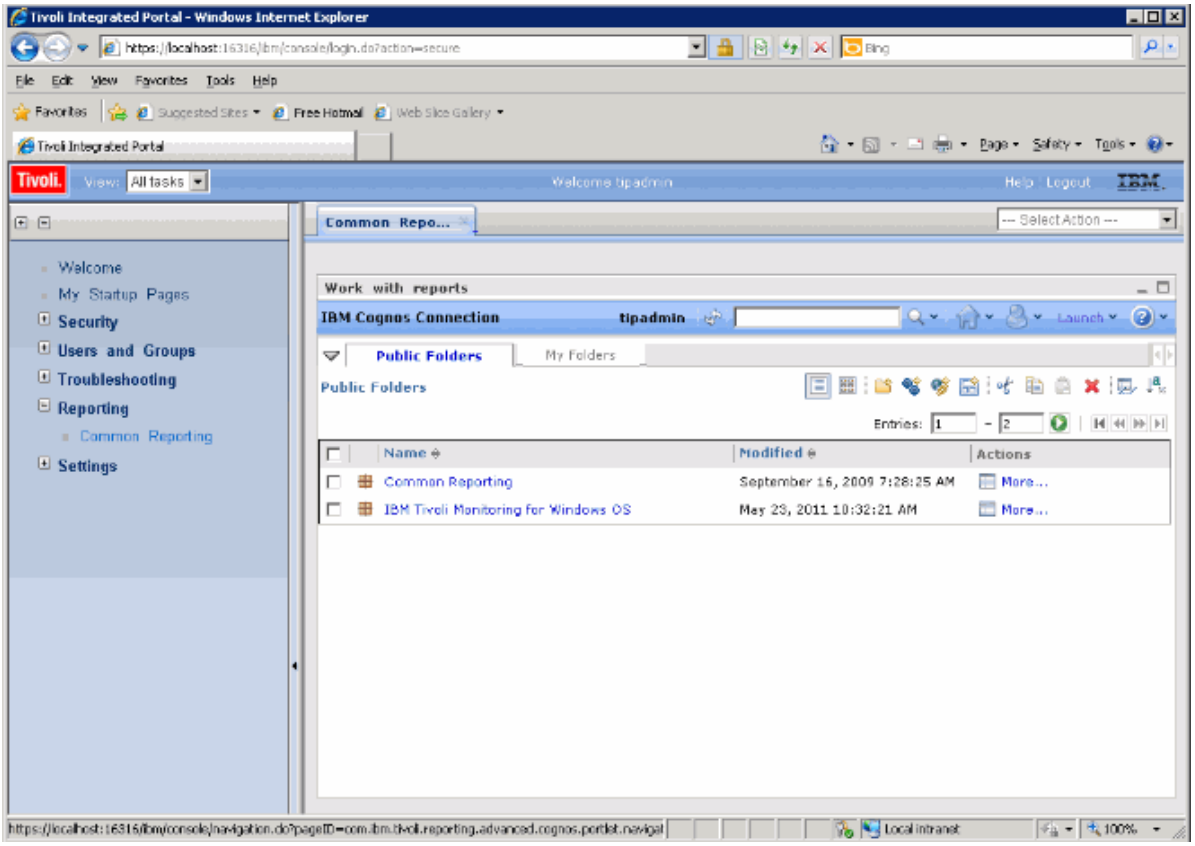


Figura 82. Selección de Common Reporting

c) Seleccione el agente de Tivoli Monitoring en la lista proporcionada.

d) Abra la herramienta de creación de informes pulsando el menú Lanzar y seleccionando **Report Studio** o **Query Studio**.

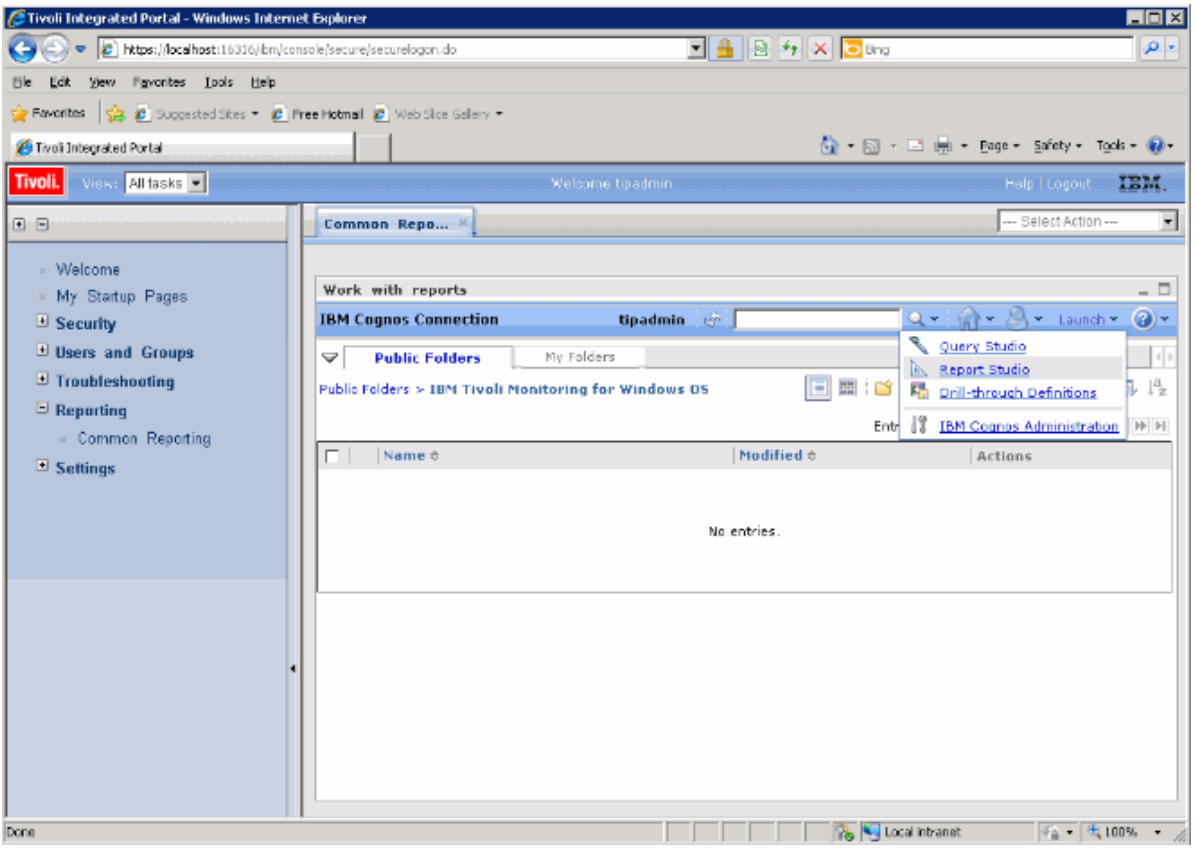


Figura 83. Selección de Report Studio

Qué hacer a continuación

Puede utilizar Report Studio para crear nuevos informes o plantillas, o puede modificar un informe o plantilla existente.

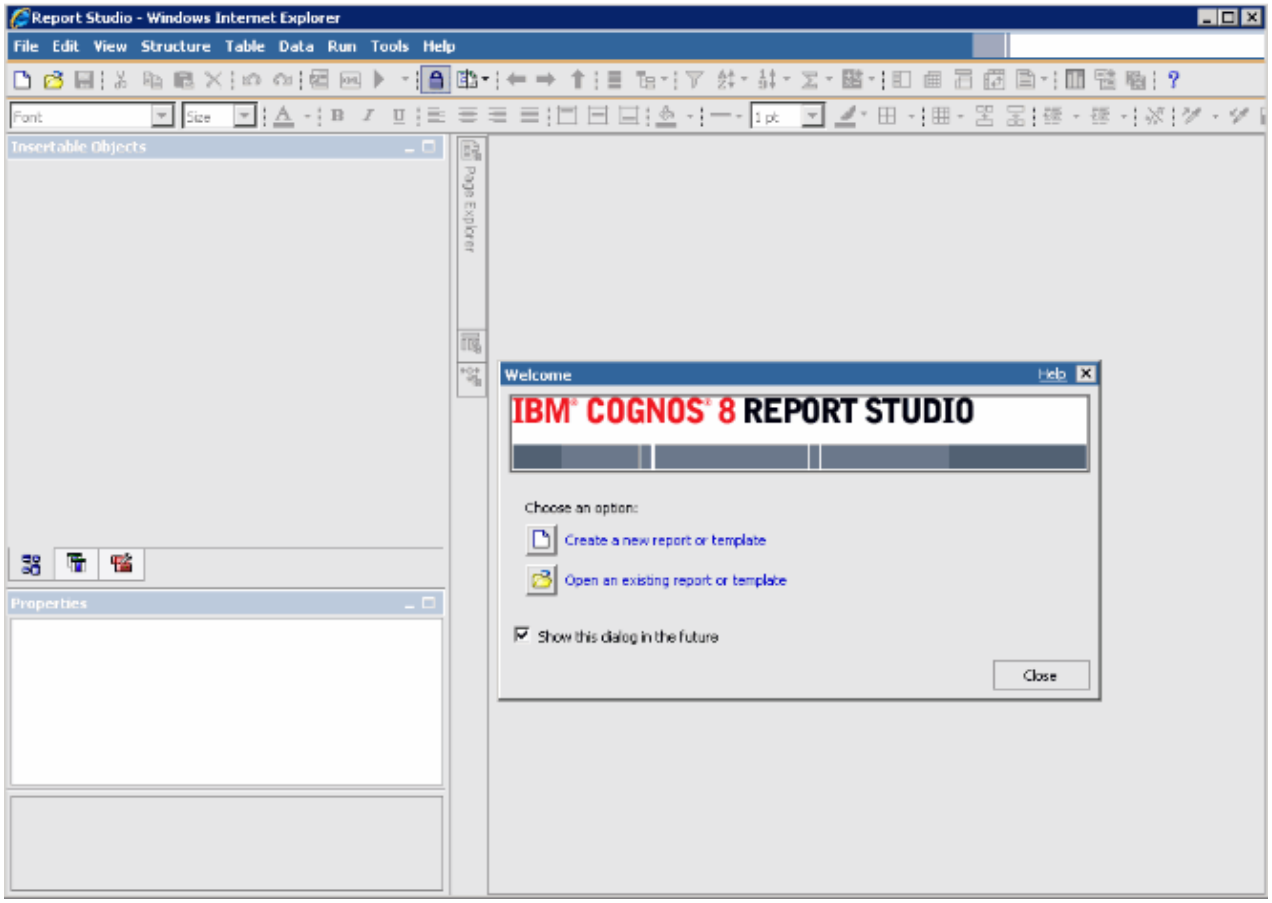


Figura 84. Report Studio

Para obtener más información, consulte la recopilación de temas de Tivoli Common Reporting en el IBM Knowledge Center.

Llenado de la tabla ManagedSystem

La tabla `ManagedSystem` se llena utilizando el procedimiento `kqz_populate_msn` almacenado.

Para obtener más información, consulte "Ejecución del procedimiento almacenado de DB2" en la página 1526. Este procedimiento se debe ejecutar periódicamente para que la tabla `ManagedSystem` contenga la lista actual de nombres de sistemas gestionados.

El procedimiento almacenado lee las tablas históricas siguientes en Tivoli Data Warehouse, si existen:

- La tabla de estado del objeto de rendimiento del agente
- La tabla de disponibilidad del agente. Los agentes que supervisan los procesos o servicios tienen una tabla de disponibilidad.
- Las tablas de descubrimiento del agente. Los agentes de subnodo crean tablas de descubrimiento.

La recopilación histórica se debe iniciar en un conjunto concreto de grupos de atributos. Se genera un conjunto de scripts que crea e inicia la recopilación histórica para dichos grupos de atributos. Si no desea utilizar los scripts, la lista de grupos de atributos se lista en el bloque de cabecera de comentario del script.

Se crean scripts de ejemplo que muestran qué tablas deben tener habilitada la recopilación histórica:

- `reports/configuretdw.sh`
- `reports/configuretdw.bat`

La tabla siguiente describe los argumentos obligatorios:

Nota: Debe especificar `-n` o `-m`, pero no ambos.

Tabla 301. Argumentos necesarios	
Argumento	**Descripción**
`-h` *`inicio_candle`*	La vía de acceso de instalación de Tivoli Monitoring.
`-u` *`usuario_teps`*	Usuario del servidor de Tivoli Enterprise Portal con el que iniciar sesión cuando crea las recopilaciones históricas.
`-n` *`nombre_tems`*	Servidor de Tivoli Enterprise Monitoring en el que se deben iniciar las recopilaciones. Se puede especificar más de un Tivoli Enterprise Monitoring Server utilizando una lista separada por espacios. Si especifica más de un servidor de Tivoli Enterprise Monitoring, ponga la lista entre comillas. Por ejemplo, `-n "tems1 tems2"`
`-m` *`grupo_sistema_gestionado_o_sistema_gestionado`*	El nombre de grupo de sistemas gestionados o de sistema gestionado en el que se debe iniciar la colección. Se puede especificar más de un grupo de sistemas o de sistema gestionados utilizando una lista separada por espacios. Si especifica más de un grupo de sistemas gestionados o de sistema gestionado, coloque la lista entre comillas. Por ejemplo, `-m "msg1 msg2"`

La tabla siguiente describe los argumentos opcionales:

Tabla 302. Argumentos opcionales	
Argumento	**Descripción**
`-s` *`host_teps`*	El nombre de host o dirección IP de Tivoli Enterprise Portal Server. Si no se especifica, el valor predeterminado es localhost.
`-p` *`contraseña_teps`*	La contraseña para el usuario de Tivoli Enterprise Portal Server que se especifica con la opción `-u`. Si no se especifica, el script solicita la contraseña
`-c` *`intervalo_recopilación_histórica`*	El intervalo de recopilación histórica a utilizar cuando se inician las recopilaciones históricas. Si no se especifica, el valor predeterminado es 1h (1 hora). Los valores válidos son: `15m`, `30m`, 1h, 12h o 1d, donde `m` es minutos, h es horas y d es días.
`-r` *`intervalo_poda`*	El intervalo de poda a utilizar para los datos históricos. Los datos históricos se deben podar para que las tablas no continúen creciendo. Si no se especifica, el valor predeterminado es 2d (2 días). Utilice d para días, `m` para meses, y para años.

Después de reiniciar la recopilación histórica, el procedimiento almacenado `kqz_populate_msn` debe ejecutarse se debe ejecutar periódicamente. El procedimiento almacenado se ejecuta periódicamente por lo que la tabla `ManagedSystem` contiene la lista más actual de sistemas gestionados del entorno de Tivoli Monitoring

Ejecución del procedimiento almacenado de DB2
Ejecución de un procedimiento almacenado en DB2.

Acerca de esta tarea

Lleva a cabo los pasos siguientes para ejecutar el procedimiento almacenado en DB2:

Procedimiento

1. Conecte a la base de datos de Tivoli Data Warehouse como el usuario warehouse:

```
connect to <alias de base de datos Tivoli Data Warehouse> user
<ID de usuario de Tivoli Data Warehouse> using <contraseña>
```

2. Ejecute el procedimiento almacenado:

```
db2 "call <esquema de Tivoli Data Warehouse>.kqz_populate_msn
('<código de producto en tres letras para el agente>')"
```

Ejecución del procedimiento almacenado de Oracle

Ejecute un procedimiento almacenado en Oracle

Acerca de esta tarea

Lleve a cabo los pasos siguientes para ejecutar el procedimiento almacenado en Oracle:

Procedimiento

1. Inicie `sqlplus`:

```
sqlplus <id de usuario de Tivoli Data
Warehouse>/<contraseña>@
<SID de Oracle>
```

2. Ejecute el procedimiento almacenado:

```
execute kqz_populate_msn('<código de producto en tres letras para el agente>');
```

Ejecución del procedimiento almacenado en SQL Server 2005 y 2008

Ejecute un procedimiento almacenado en SQL Server.

Acerca de esta tarea

Lleve a cabo los pasos siguientes para ejecutar el procedimiento almacenado en SQL Server 2005 y 2008:

Procedimiento

Ejecute el procedimiento almacenado:

```
osql -S <servidor> -U <ID de Tivoli Data Warehouse> -P
<contraseña de Tivoli Data Warehouse> -d
<nombre de base de datos de Tivoli Data Warehouse> -Q "EXEC
[<esquema de Tivoli Data Warehouse>].[kqz_populate_msn]
@pv_productcode = N'<código de tres letras del producto>'"
```

Exportación de informes y modelos de datos de Tivoli Common Reporting

Exporte informes y modelos de datos de Tivoli Common Reporting.

Procedimiento

1. Inicie la sesión en Tivoli Common Reporting.
2. Vaya a Carpetas públicas y bajo **Reporting** en el panel de navegación, seleccione **Common Reporting**.
3. En la sección Trabajar con informes, pulse el menú **Iniciar** y seleccione **Administración de IBM Cognos**.
4. Pulse en el separador **Configuración**.

5. Pulse **Administración de contenidos**.

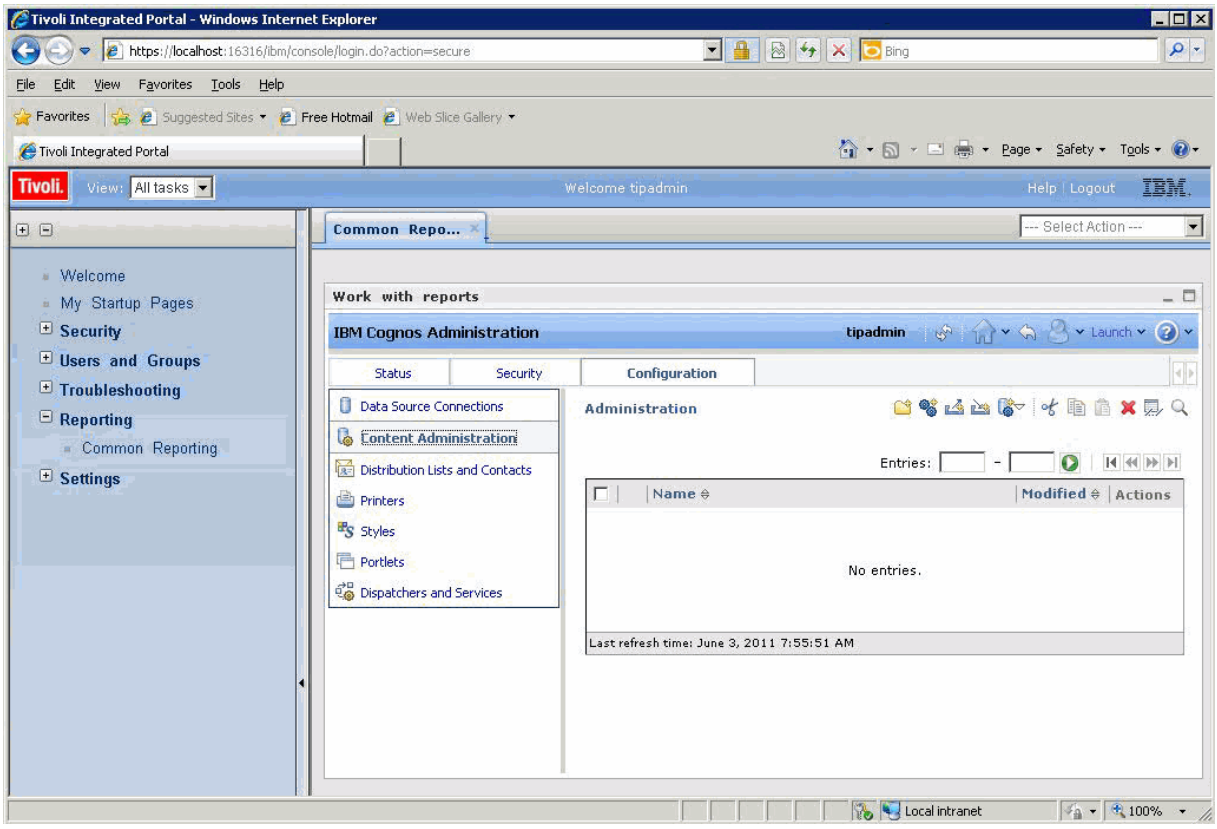


Figura 85. Separador Administración de contenido

6. Pulse el icono **Nueva exportación** para exportar un nuevo paquete.
7. Asigne un nombre al paquete. Si lo prefiere, puede añadir una sugerencia de pantalla y una descripción.
8. Marque **Seleccionar carpetas públicas y contenido de directorio** .
9. En el diálogo Carpetas públicas, pulse el enlace **Añadir**.
10. Mueva su paquete de agente a **Entradas seleccionadas**.
11. En la última página del asistente, seleccione **Guardar solo**. Cuando se completa el asistente, el paquete de informes se lista en el separador Administración de contenidos.
12. En el separador Administración de contenidos, pulse la flecha verde (Ejecutar) para crear el archivo comprimido `.zip`.

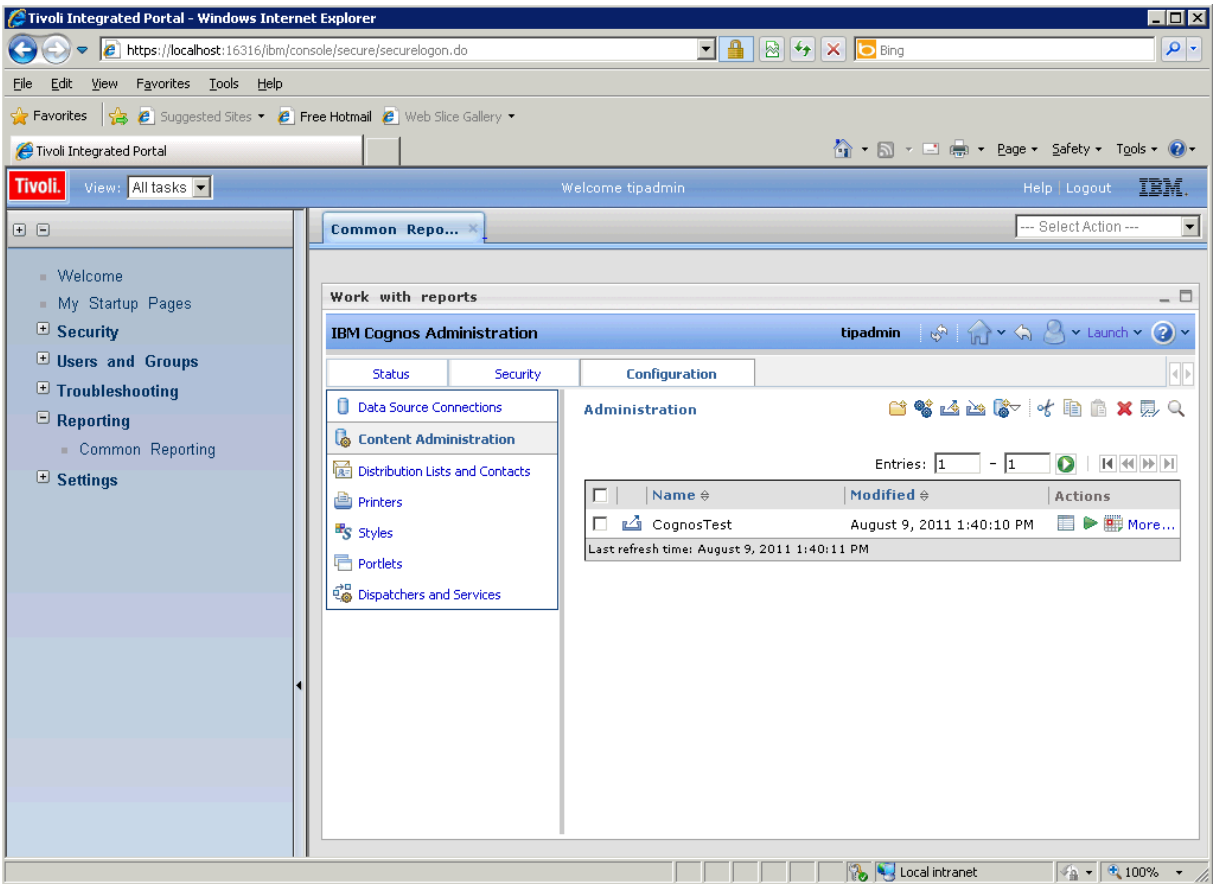


Figura 86. Separador Administración de contenidos que lista el paquete de agente

Resultados

El archivo comprimido `.zip` que el proceso de exportación crea se coloca en el directorio de despliegue.

- La vía de acceso al directorio para Tivoli Common Reporting versión 1.3 es:

```
C:\IBM\tivoli\tip\products\tcr\Cognos\c8\deployment
```

- La vía de acceso al directorio para Tivoli Common Reporting versión 2.1 o posterior es:

```
C:\IBM\tivoli\tipv2Components\TCRComponent\cognos\deployment
```

Qué hacer a continuación

Para obtener más información sobre la exploración de informes, consulte Exploración de paquetes de informes de Cognos en *Tivoli Common Reporting: Guía del usuario*.

Importación de informes en Agent Builder

Cuando se exporta el paquete de informe desde Tivoli Common Reporting, se puede importar al proyecto de Agent Builder. Después, el paquete de informe puede incluirse en la imagen de instalación del agente.

Procedimiento

1. Pulse el botón derecho del ratón sobre el proyecto del agente en Agent Builder.
2. Seleccione **IBM** > **Importar paquete de informes**.
3. En la ventana **Importar paquete de informes**, seleccione el **Tipo de base de datos** en el que se ha creado el paquete de informes.
4. Especifique la vía de acceso completa al paquete de informes o pulse **Examinar** para seleccionarlo.
5. Pulse **Aceptar**.

6. El paquete de informe se muestra ahora en el proyecto de agente bajo el directorio `reports/`*`tipo_bd`*.

   Nota: Si crea paquetes de informes que son específicos de base de datos, debe importar cada paquete a Agent Builder.

Instalación de informes desde un paquete de agente en Tivoli Common Reporting
Importe un paquete de informe desde el agente a Tivoli Common Reporting

Procedimiento

1. Siga los pasos del asistente para importar un nuevo paquete desde la imagen del agente.

   En la imagen del agente, los informes se encuentran en: `reports/`*`Tipo_bd`*`/K`*`xx`*`/reports/cognos_reports/itmk`*`xx`*`/packages`
2. Copie el archivo `zip` comprimido de informes en el directorio de despliegue de Tivoli Common Reporting.
   - La vía de acceso del directorio para Tivoli Common Reporting versión 1.3 es: `C:\IBM\tivoli\tip\products\tcr\Cognos\c8\deployment`
   - La vía de acceso del directorio para Tivoli Common Reporting versión 2.1 o posterior es: `C:\IBM\tivoli\tipv2Components\TCRComponent\cognos\deployment`
3. Inicie la sesión en Tivoli Common Reporting.
4. Vaya a Carpetas públicas y bajo **Reporting** en el panel de navegación, seleccione **Common Reporting**.
5. En la sección Trabajar con informes, pulse el menú **Iniciar** y seleccione **Administración de IBM Cognos**.
6. Vaya al separador **Configuración** y abra la sección **Administración de contenido**.
7. Pulse **Nueva importación** para crear una importación de paquete.
8. Seleccione el paquete de informes del agente.
9. Seleccione las carpetas públicas que desea importar.
10. Seleccione Guardar.
11. Pule la flecha (ejecutar) verde para importar.

Resultados

Para obtener más información, consulte Inicio de sesión en la interfaz de generación de informes en la publicación *Tivoli Common Reporting: Guía del usuario*.

Expresiones regulares de ICU

Una descripción de los detalles de la implementación de expresiones regulares de ICU.

Este contenido de referencia se extrae de *ICU User Guide*. El contenido describe los detalles de la implementación de expresiones regulares de ICU. Esta información resulta esencial si utiliza la función de expresión regular de Agent Builder, ya que los distintos lenguajes de programación implementan las expresiones regulares de forma ligeramente diferente.

Tabla 303. Metacaracteres de expresiones regulares

Carácter	Descripción
\a	Coincide con BELL, \u0007
\A	Coincide con el principio de la entrada. Difiere de ^ en que \A no coincide tras una línea nueva dentro de la entrada.

Tabla 303. Metacaracteres de expresiones regulares (continuación)	
Carácter	**Descripción**
\b, fuera de [Set]	Coincide si la posición actual es un límite de palabra. Los límites aparecen en las transiciones entre caracteres de palabra (\w) y caracteres que no son palabra (\W), omitiendo las marcas de combinación. Para obtener más información sobre límites de palabra, consulte el manual ICU Boundary Analysis.
\b, dentro de [Set]	Coincide con BACKSPACE, \u0008.
\B	Coincide si la posición actual no es una palabra.
\cX	Coincide con un carácter Control-X.
\d	Coincide con cualquier carácter de la categoría de Unicode general Nd (Número, Dígito decimal.)
\D	Coincide con cualquier carácter que no sea un dígito decimal.
\e	Coincide con ESCAPE, \u001B.
\E	Termina una secuencia de entrecomillado \Q ... \E.
\f	Coincide con FORM FEED, \u000C.
\G	Coincide si la posición actual está al final de la coincidencia anterior.
\n	Coincide con LINE FEED, \u000A.
\N{UNICODE CHARACTER NAME}	Coincide con el carácter especificado.
\p{UNICODE PROPERTY NAME}	Coincide con cualquier carácter que tenga la propiedad Unicode especificada.
\P{UNICODE PROPERTY NAME}	Coincide con cualquier carácter que no tenga la propiedad Unicode especificada.
\Q	Coloca comillas alrededor de todos los siguientes caracteres hasta \E.
\r	Coincide con CARRIAGE RETURN, \u000D.
\s	Coincide con un carácter de espacio en blanco. El espacio en blanco se define como [\t\n\f\r \p{Z}].
\S	Coincide con un carácter que no sea de espacio en blanco.
\t	Coincide con HORIZONTAL TABULATION, \u0009.
\uhhhh	Coincide con el carácter que tiene el valor hexadecimal hhhh.
\Uhhhhhhhh	Coincide con el carácter que tiene el valor hexadecimal hhhhhhhh. Se deben especificar exactamente ocho dígitos hexadecimales, aunque el punto de código Unicode más largo sea \U0010ffff.

Tabla 303. Metacaracteres de expresiones regulares (continuación)	
Carácter	**Descripción**
\w	Coincide con un carácter de palabra. Los caracteres de palabra son [\p{Ll}\p{Lu} \p{Lt}\p{Lo}\p{Nd}].
\W	Coincide con un carácter que no sea de palabra.
\x{hhhh}	Coincide con el carácter que tiene el valor hexadecimal hhhh. Se pueden especificar entre uno y seis dígitos hexadecimales.
\xhh	Coincide con el carácter que tiene el valor hexadecimal de 2 dígitos hh.
\X	Coincide con un clúster Grapheme.
\Z\	Coincide si la posición actual está al final de la entrada, pero antes del terminador de línea final, si existe.
\z	Coincide si la posición actual está al final de la entrada.
\n	Referencia anterior. Coincide con la coincidencia de grupo de captura número n. n debe ser un número > 1 y < el número total de grupos de captura del patrón. **Nota:** Los valores de escape octal, como \012, no reciben soporte en las expresiones regulares de ICU.
[pattern]	Coincide con cualquier carácter 1 del conjunto. Consulte UnicodeSet para obtener una descripción completa de lo que puede aparecer en el patrón
.	Coincide con cualquier carácter.
^	Coincide con el principio de una línea.
$	Coincide con el final de una línea.
\	Coloca comillas alrededor del siguiente carácter. Los caracteres que deben estar incluidos entre comillas para ser tratados como literales son * ? + [( ) { } ^ $ | \ . /

Tabla 304. Operadores de expresiones regulares	
Operador	**Descripción**
|	Alterne. A | B coincide con A o B.
*	Coincide 0 o más veces. Coincide tantas veces como sea posible.
+	Coincide 1 o más veces. Coincide tantas veces como sea posible.
?	Coincide con cero o 1 vez . Es preferible una.

Tabla 304. Operadores de expresiones regulares (continuación)	
Operador	**Descripción**
{n}	Coincide exactamente n veces
{n,}	Coincide al menos n veces. Coincide tantas veces como sea posible.
{n,m}	Coincide entre n y m veces. Coincide tantas veces como sea posible, pero no más de m.
*?	Coincide 0 o más veces. Coincide tantas pocas veces como sea posible.
+?	Coincide 1 o más veces. Coincide tantas pocas veces como sea posible.
??	Coincide con cero o 1 vez . Es preferible cero.
{n}?	Coincide exactamente n veces
{n,}?	Coincide al menos n veces, pero no más de lo necesario para una coincidencia de patrón general
{n,m}?	Coincide entre n y m veces. Coincide tan pocas veces como sea posible, pero no menos de n.
*+	Coincide 0 o más veces. Coincide tantas veces como sea posible cuando se encuentra la primera, no se reintenta con menos aunque la comparación general no tenga éxito (coincidencia posesiva).
++	Coincide 1 o más veces. Coincidencia posesiva.
?+	Coincide con cero o 1 vez . Coincidencia posesiva.
{n}+	Coincide exactamente n veces
{n,}+	Coincide al menos n veces. Coincidencia posesiva.
{n,m}+	Coincide entre n y m veces. Coincidencia posesiva.
(...)	Paréntesis de captura. Rango de entrada que ha coincidido con la subexpresión entre paréntesis si está disponible tras la coincidencia.
(?: ...)	Paréntesis que no es de captura. Agrupa el patrón incluido, pero no proporciona captura para el texto coincidente. Es más eficiente que la captura de paréntesis.
(?> ...)	Paréntesis de coincidencia atómica. La primera coincidencia de la subexpresión entre paréntesis es la única que se intenta. Si no lleva a una coincidencia de patrón general, realice una copia de seguridad de la búsqueda de una coincidencia con una posición delante de "(?>"
(?# ...)	Comentario en formato libre (?# comment).
(?= ...)	Aserción de búsqueda anticipada. Es verdadera si el patrón entre paréntesis coincide en la posición de entrada actual, pero no avanza la posición de entrada.

Tabla 304. Operadores de expresiones regulares (continuación)	
Operador	**Descripción**
`(?! ... )`	Aserción de búsqueda anticipada negativa. Es verdadera si el patrón entre paréntesis no coincide en la posición de entrada actual. No avanza la posición de entrada.
`(?<= ... )`	Aserción de búsqueda con retrocesión. Es verdadera si el patrón entre paréntesis coincide con el texto que precede a la posición de entrada actual. El último carácter de la coincidencia es el carácter de entrada antes de la posición actual. No modifica la posición de entrada. La longitud de cadenas posibles que coinciden con el patrón de búsqueda con retrocesión no debe ser ilimitada (sin operadores * o +.)
`(?<!...)`	Aserción de búsqueda con retrocesión negativa. Es verdadera si el patrón entre paréntesis no coincide con el texto que precede la posición de entrada actual. El último carácter de la coincidencia es el carácter de entrada antes de la posición actual. No modifica la posición de entrada. La longitud de cadenas posibles que coinciden con el patrón de búsqueda con retrocesión no debe ser ilimitada (sin operadores * o +.)
`(?ismx-ismx: ... )`	Valores de distintivo. Evalúa la expresión entre paréntesis con los distintivos especificados habilitados o inhabilitados.
`(?ismx-ismx)`	Valores de distintivo. Cambia los valores de distintivo. Los cambios se aplican a la parte del patrón que sigue al valor. Por ejemplo, `(?i)` cambia a una coincidencia que no es sensible a mayúsculas y minúsculas.

Texto de sustitución

El texto de sustitución para operaciones de búsqueda y sustitución puede contener referencias a texto de grupo de captura de la búsqueda. Las referencias son de tipo $n, donde n es el número del grupo de captura.

Tabla 305. Caracteres del texto de sustitución	
Carácter	**Descripción**
$n	El texto del grupo de capturas posicional n se sustituye por `$n.` n debe ser `= 0`, y no mayor que el número de grupos de captura. Un símbolo $ que no va seguido de un dígito no tiene ningún significado especial, y se visualiza en el texto de sustitución como sí mismo, un símbolo $.

Tabla 305. Caracteres del texto de sustitución (continuación)	
Carácter	**Descripción**
\	Trata este carácter como un literal, suprimiendo cualquier significado especial. El signo de escape en barras inclinadas invertidas solo se necesita en texto de sustitución para `'$'` y `'\'`, pero se puede utilizar en cualquier otro carácter sin efectos adversos.
$@n	El texto del grupo de captura n se sustituye por la expresión regular que ha coincidido con el grupo de captura n. n debe ser >= 0 y no mayor que el número de grupos de captura. Un símbolo $@ que no va seguido de un dígito no tiene ningún significado especial, y se visualiza en el texto de sustitución como sí mismo, un símbolo $@.
$#n	El texto del grupo de captura coincidente n se sustituye por $#n. n debe ser >= 0, y no mayor que el número de grupos de captura coincidentes. Un símbolo $# que no va seguido de un dígito no tiene ningún significado especial, y se visualiza en el texto de sustitución como sí mismo, un símbolo $#.

Opciones de distintivo

Los siguientes distintivos controlan diversos aspectos de la coincidencia de expresión regular. Los valores de distintivo se pueden especificar en el momento que una expresión se compila en un objeto RegexPattern. O bien, pueden especificarse dentro del propio patrón utilizando las opciones de patrón `(?ismx-ismx)`.

Tabla 306. Opciones de distintivo		
Distintivo (patrón)	**Distintivo (constante de API)**	**Descripción**
i	UREGEX_CASE_INSENSITIVE	Si está definido, la coincidencia se realiza teniendo en cuenta mayúsculas y minúsculas.
x	UREGEX_COMMENTS	Si está establecido, puede utilizarse un espacio en blanco y #comments dentro de patrones.
s	UREGEX_DOTALL	Si está establecido, un signo "." en un patrón coincide con un terminador de línea en el texto de entrada. De forma predeterminada no es así. Un par retorno de carro / salto de línea en texto se comporta como un terminador de una sola línea y coincide con un solo "." en un patrón de RE

Tabla 306. Opciones de distintivo (continuación)		
Distintivo (patrón)	**Distintivo (constante de API)**	**Descripción**
m	UREGEX_MULTILINE	Controla el comportamiento de "^" y "$" en un patrón. De forma predeterminada, estos patrones solo coinciden a l principio y al final, respectivamente, del texto de entrada. Si este distintivo está establecido, "^" y "$" también coinciden al principio y al final de cada línea dentro del texto de entrada.

Creación de paquetes de archivos sin agente

Puede crear paquetes de archivos que se pueden colocar en el depósito de Tivoli Monitoring. Estos paquetes de archivos se pueden luego desplegar en sistemas de destino del entorno.

Acerca de esta tarea

Con esta función, puede configurar remotamente los productos para los que no hay ninguna opción de configuración remota. Para utilizar esta función, se colocan los archivos de configuración llenados previamente en el depósito y se envían a los sistemas deseados.

Procedimiento

1. En Agent Builder, seleccione **Archivo** > **Nuevo** > **Otro**.
2. En **Agent Builder**, seleccione **Paquete de despliegue remoto sin agente**.
3. Pulse **Siguiente**.
4. En el campo **Nombre de proyecto**, especifique un nombre para el proyecto.
5. Pulse **Siguiente**.
6. Complete la información de la ventana **Información de paquete de despliegue remoto**:
   a) En el campo **Identificador de paquete**, escriba un identificador que sea una cadena alfanumérica exclusiva entre 3 y 31 caracteres. Esta cadena puede contener un guión. La cadena debe empezar por una letra pero no puede empezar por una K o un guión.
   b) En el campo **Descripción de paquete**, escriba una descripción del paquete.
   c) En el campo **Versión**, escriba una versión para el paquete con el formato VVRRMMAAA. Donde `vv`= número de versión; `rr`= número de release; `mm`= número de modificación (número de fixpack) y `fff` = número de arreglo temporal.
7. En el área **Sistemas operativos**, seleccione los sistemas operativos en los que se puede desplegar el paquete.
8. Pulse **Finalizar** para crear un proyecto en el espacio de trabajo y abra el **Editor de paquetes de despliegue remoto**.

Editor de paquete de despliegue remoto

El Editor de paquete de despliegue remoto se utiliza para generar mandatos que sirven para desplegar el paquete de archivos.

El Editor de paquete de despliegue remoto proporciona información sobre el paquete de un proyecto.

La sección **Información de identificación de paquete** contiene la siguiente información:

Identificador de paquete
ID exclusivo del paquete

Descripción de paquete
Descripción del paquete

Versión de paquete
Versión del paquete

Compilación
Identificador de compilación para el paquete. Especifique aquí un número de compilación. Si no se especifica ningún número de compilación, se generará un número a partir de la fecha y la hora en la que se generó el paquete.

Recuadro de selección Crear mandatos de copia para los archivos del paquete
Pulse el recuadro de selección para generar un conjunto de mandatos de copia predeterminados que se ejecuten al desplegarse el paquete. Los archivos se copian en la ubicación especificada en el recuadro de texto **Copiar ubicación**. La ubicación predeterminada es *INSTALLDIR*. Especifique esta variable de despliegue desde el despliegue de línea de mandatos mediante la definición de KDY.*INSTALLDIR*=...

La sección **Sistemas operativos** muestra los sistemas operativos en los que se puede desplegar el paquete.

La sección **Mandatos** muestra los mandatos que ejecutar al desplegar el paquete.

La sección **Paquetes de requisito previo** muestra los paquetes que deben estar presentes para que funcione este paquete.

Utilice el Editor de paquete de despliegue remoto para elegir un conjunto predeterminado de mandatos de copia que copian los archivos del paquete en una ubicación establecida. Si se selecciona esta opción, se genera un mandato de copia para cada archivo del proyecto de paquete. La ubicación de copia predeterminada es *INSTALLDIR*. Una variable de despliegue remota especial que, si no se establece en la línea de mandatos de despliegue, regresa al valor predeterminado *CANDLEHOME*. Para modificación la ubicación que se especifica *INSTALLDIR*, especifique la propiedad **KDY.INSTALLDIR** cuando ejecute el mandato **addSystem**.

La misma estructura de directorio especificada en el proyecto de paquete se duplica en *INSTALLDIR*. Por ejemplo, si hay una carpeta denominada `config` en el proyecto de paquete con un archivo denominado `myprod.config`, el mandato de copia generado copia el archivo en *INSTALLDIR*`/config/myprod.config` cuando se despliega el paquete.

Adición de mandatos al paquete

Puede especificar mandatos adicionales para que se ejecuten durante el despliegue.

Acerca de esta tarea

Puede especificar más mandatos para que se ejecuten durante el despliegue al utilizar el **Editor de paquete de despliegue remoto**.

Procedimiento

1. Para especificar más mandatos para que se ejecuten durante el despliegue, pulse **Añadir** en la sección **Mandatos** del **Editor de paquete de despliegue remoto**.
2. En la ventana **Mandato**, seleccione el tipo de mandato **Instalación previa**, **Instalación**, **Posterior a la instalación** o **Desinstalación** y después especifique el mandato a ejecutar.

   Debe especificar la vía de acceso completamente calificada al mandato que desee ejecutar. Para su comodidad, el despliegue remoto proporciona un conjunto de variables predefinidas. Para consultar la variable para un mandato, especifique la variable entre barras verticales, por ejemplo, `|DEPLOYDIR|`. Para obtener más información sobre las variables predefinidas para mandatos, consulte (Tabla 307 en la página 1538).

Tabla 307. Variables predefinidas para mandatos	
Variable	**Descripción**
DEPLOYDIR	El directorio temporal del punto final en el que el paquete se almacena durante el despliegue. Por ejemplo, si desea ejecutar `myscript.sh`, script que se incluye en el paquete, especifique el siguiente mandato: `|DEPLOYDIR|/myscript.sh`
INSTALLDIR	*CANDLEHOME* o el valor de *KDY.INSTALLDIR* si se especifica en el mandato **addSystem**.
CANDLEHOME	El directorio de instalación de Tivoli Monitoring.

3. Por último, seleccione los **Sistemas operativos** en los que se va a ejecutar el mandato.

Adición de requisitos previos al paquete

Utilice el **Editor de paquete de despliegue remoto** para especificar requisitos previos para el paquete.

Procedimiento

1. Para añadir un requisito previo, pulse **Añadir** en la sección **Paquetes de requisito previo** del **Editor de paquete de despliegue remoto**, página **Información de paquete**.
2. En la ventana **Nuevo requisito previo**, especifique el identificador de paquete del que depende el paquete y la versión mínima necesaria.
3. Seleccione los sistemas operativos para los que se necesita este requisito previo.
4. Pulse **Aceptar** para finalizar y salir.

Adición de archivos al paquete

Añada archivos a un paquete de archivos utilizando el **Editor de paquete de despliegue remoto**.

Procedimiento

1. Para añadir archivos a un paquete de despliegue remoto, siga uno de los procedimientos siguientes:
   - En el Editor de paquete, pulse **Añadir archivos al paquete**.
   - Pulse con el botón derecho del ratón el árbol de Navigator y, a continuación, pulse **Despliegue remoto de IBM Tivoli Monitoring** > **Añadir archivos a paquete**.

   Ambas acciones muestran la ventana **Importar archivos de paquete**:
2. Especifique archivos individuales o directorios que contengan archivos en el área **Información de archivo**.
3. Pulse **Finalizar**.

   Los archivos o directorios que se especifican se copian en el directorio del proyecto. La estructura de directorios en el proyecto se mantiene al crear el paquete de despliegue remoto. Si desea que Agent Builder genere mandatos de copia predeterminados, asegúrese de que los archivos estén en la estructura de directorio correcta para el despliegue.

Generación del paquete

Utilice el Agent Builder para generar un paquete para el despliegue remoto de un agente.

Procedimiento

1. Para generar el paquete de despliegue remoto, siga uno de los procedimientos siguientes para visualizar la ventana **Generar paquete de despliegue remoto final**

- En el **Editor de paquete de despliegue remoto**, pulse **generar el paquete de despliegue remoto final**.
- Pulse con el botón derecho del ratón sobre el proyecto en el árbol de Navigator, luego pulse **Despliegue remoto de IBM Tivoli Monitoring** > **Generar paquete de despliegue remoto**

2. Ahora puede generar el paquete de dos maneras:
   - Si hay un servidor de Tivoli Enterprise Monitoring Server en el sistema en el que esté ejecutando Agent Builder, pulse **Instalar el paquete de despliegue remoto en un depósito de TEMS local**.

     Agent Builder intentará determinar la ubicación de instalación de Tivoli Monitoring la introducirá en el campo **Directorio**. Si *CANDLE_HOME* no se ha establecido, se utiliza la ubicación predeterminada `C:\IBM\ITM` o `/opt/IBM/ITM`. Asegúrese de que la ubicación de instalación es correcta antes de continuar.

     Debe proporcionar la información de inicio de sesión de Tivoli Enterprise Monitoring Server para instalar el paquete.
   - Para generar el paquete en un directorio del sistema, pulse **Generar el paquete de despliegue remoto en un directorio local**

     Una vez finalizado el proceso, deberá transferir este directorio a un sistema de Tivoli Enterprise Monitoring Server y utilizar el mandato `tacmd addbundles` para añadir el paquete al depósito.

Qué hacer a continuación

Cuando despliega el paquete, debe utilizar el mandato `tacmd addSystem`. Por ejemplo:

```
tacmd addsystem -t MONITORINGCOLLECTION -n Primary:ITMAGT:NT
```

Donde `-t` (tipo) es el código de producto tal como lo devuelve el mandato `tacmd viewDepot`:

```
>tacmd viewDepot
Código de producto: MONITORINGCOLLECTION
Versión : 010000003
Descripción : MonitoringCollectionScripts
Tipo de host: WINNT
Versión de host: WINNT
Requisitos previos:
```

Nota: No puede realizar un despliegue de forma remota desde el escritorio o navegador de Tivoli Enterprise Portal. El despliegue remoto desde el escritorio o navegador de Tivoli Enterprise Portal da como lugar el mensaje KFWITM219E.

Consulte la documentación de Tivoli Monitoring para obtener información más detallada.

Creación de paquetes desplegables para analizadores de Tivoli Netcool/OMNIbus

Puede utilizar Agent Builder para crear paquetes de empaquetado y configuración que se puedan utilizar para desplegar pruebas de Tivoli Netcool/OMNIbus en sistemas remotos.

Acerca de esta tarea

Para dar soporte al despliegue remoto de pruebas, también puede crear paquetes de Tivoli Netcool/OMNIbus que se puedan desplegar en los sistemas remotos antes de desplegar las pruebas.

Procedimiento

1. En Agent Builder, seleccione **Archivo** > **Nuevo** > **Otro**.
2. En **Asistentes de IBM Tivoli OMNIbus**, seleccione **Paquete de paquetes**.
3. Pulse **Siguiente**.

Qué hacer a continuación

A continuación, utilice el asistente de **Paquete de instalación de OMNIbus** para crear los paquetes. Para obtener información sobre cómo utilizar este asistente, consulte la documentación de Tivoli Netcool/OMNIbus.

Soporte de nombres de archivo dinámicos

Utilice el soporte de nombres de archivo dinámicos para especificar un patrón de nombre de archivo en lugar de un nombre de archivo real.

Algunos programas de aplicación crean un nombre de archivo de salida que está sujeto a cambios. El nombre cambia en función de criterios específicos como el día, mes o año actual, o un nombre de archivo que incluye un número de secuencia incremental. En estos casos, puede especificar el patrón de nombre de archivo e lugar del nombre de archivo real. Existen dos formatos de patrón que se reconocen al especificar el patrón del nombre de archivo:

- Expresiones regulares (preferido).
- Sintaxis de nombres de archivo dinámicos de IBM Tivoli Universal Agent (en desuso).

Patrones de nombres de archivo de expresiones regulares

Para especificar patrones de nombres de archivo, puede utilizar expresiones regulares según la sintaxis ICU (International Components for Unicode) que se documenta en el "Expresiones regulares de ICU" en la página 1530. Para utilizar esta capacidad, debe marcar el recuadro de selección **Los nombres de archivos coinciden con expresiones regulares** en la página **Información avanzada de grupo de atributos de archivo de registro**. Al especificar patrones de expresiones regulares, también debe seleccionar una opción en la lista **Cuando coinciden varios archivos** de la página **Información avanzada de grupo de atributos de archivo de registro** para especificar las directrices para seleccionar el archivo coincidente más actual.

Nota: Las expresiones regulares son el método preferido para especificar patrones de nombres de archivos.

Para obtener más información sobre cómo configurar propiedades avanzadas de atributos de archivo de registro, consulte "Supervisión de un archivo de registro" en la página 1300, paso "6" en la página 1301. Por ejemplo, si ha especificado un patrón de nombre de archivo:

```
d:\program files\logs\tivoli.*
```

Este patrón busca nombres de archivo que empiezan por `tivoli` en el directorio `d:\program files\logs`. Las expresiones regulares se pueden especificar sólo para la parte de nombre de archivo, no para el nombre de vía de acceso.

Sintaxis de nombres de archivos dinámicos

Con la sintaxis de nombres de archivo dinámicos, sólo se puede supervisar un archivo cada vez. El proveedor de datos de archivo inspecciona todos los archivos de la ubicación de vía de acceso asignada, buscando los archivos que coincidan con el patrón definido. El proveedor de datos de archivo siempre supervisa el archivo coincidente más actual que se basa en el nombre de archivo coincidente que tenga el número o valor de fecha/hora más alto. El archivo adecuado que supervisar viene determinado por el nombre de archivo, en lugar de por la creación de archivo u otros criterios.

Se pueden especificar patrones para nombres de archivo con cualquier número de partes. Por ejemplo, `Log{###}` coincide con nombres de archivo de una parte, como `Log010` o `Log456`. En nombres de archivo de varias partes, se pueden especificar caracteres de patrón en cualquier parte del nombre de archivo o en varias partes. Por ejemplo, `aaa.bbb{???}.ccc` es un patrón válido y `aaa.bbb{???}.ccc{###}` también es válido.

Nota: Las expresiones regulares son el método preferido, más que la sintaxis de nombres de archivo dinámicos, para especificar patrones de nombre de archivo. Para obtener más información sobre las

expresiones regulares, consulte “Patrones de nombres de archivo de expresiones regulares” en la página 1540

Los siguientes ejemplos ilustran la especificación de patrón de nombre de archivo:

{########}.abc
Coincide con nombres de archivo numéricos de longitud 8 y la extensión de archivo *.abc*, como 10252006.abc o 10262006.abc. El archivo 10262006.abc se supervisa porque 10262006 es mayor que 10252006.

{########}.*
Coincide con nombres de archivo numéricos de longitud 8 e ignora la extensión de archivo. Entre los ejemplos se incluyen 20061025.log, 20061101.log y 10252006.abc. El archivo 20061101.log se supervisa porque 20061101 es el número más grande.

{######??}.abc
Coincide con nombres de archivo numéricos de longitud 8 y la extensión de archivo .abc, e ignora las dos últimas posiciones de la parte del nombre. Entre los ejemplos se incluyen 02110199.abc, 02110200.abc y 021101AZ.abc. El archivo 02110200.abc se supervisa porque 021102 es el número más grande.

Console.{######}
Coincide con nombres de archivo que contienen *Console* en la parte del nombre y un número de seis dígitos en la parte de la expresión. Entre los ejemplos se incluyen Console.000133, Console.000201 y Console.000134. El archivo Console.000201 se supervisa.

IN{######}.log
Coincide con nombres de archivo que empiezan por IN seguido de seis números y la extensión de archivo .log. Entre los ejemplos se incluyen IN021001.log, IN021002.log y IN021004.log. Se supervisa el archivo IN021004.log.

PS{###}FTP.txt
Coincide con nombres de archivo que empiezan por PS seguido de tres números, seguidos por FTP y la extensión .txt. Entre los ejemplos se incluyen PS001FTP.txt, PS005FTP.txt y PS010FTP.txt. El archivo PS010FTP.txt se supervisa.

Siga estas directrices para establecer patrones de nombres de archivo:

- Utilice llaves {} para encerrar los caracteres de patrón en un nombre de archivo. La presencia de caracteres de patrón dentro de llaves indica que se utiliza un patrón de nombre de archivo.
- Utilice un asterisco (*) como carácter comodín para ignorar extensiones de archivo o los caracteres de cola del nombre de archivo. Por ejemplo, Myapp{###}.log* especifica que cualquier nombre que empiece por Myapp, seguido de tres dígitos y de .log es una coincidencia, independientemente de lo que vaya después.

  El asterisco se debe especificar después de las llaves ({ }) y no se puede utilizar al principio de un nombre de archivo. Cuando utiliza el asterisco en una extensión de nombre de archivo, el asterisco debe utilizarse solo.

  Ejemplos de uso correcto del comodín (*):

  err{??}.*

  error{$}.*

  Ejemplos del uso incorrecto del comodín (*):

  error.20*
  Ninguna llave precede al asterisco (*).

  error*.{###}
  El asterisco no se utiliza al final del nombre de archivo.

  error.*
  Ninguna llave precede al asterisco (*).
- Si se define una extensión de archivo específica, sólo se tendrán en cuenta los archivos con la misma extensión.

- Utilice un signo de número para indicar cada elemento numérico de un nombre de archivo.
- Utilice un signo de interrogación para excluir cada elemento del convenio de denominación que no sirva como criterio de búsqueda a la hora de determinar el nombre de archivo correspondiente.
- Utilice un signo de dólar ($) para representar cualquier carácter o ningún carácter. Por ejemplo, si desea la coincidencia con dos archivos llamados Log y LogA, especifique Log{$}. El signo de dólar tiene varias restricciones de uso. Cuando utiliza uno o más signos de dólar como prefijo de un nombre de archivo como, por ejemplo, {$$$$$$}_abc.log, el número de signos de dólar debe coincidir exactamente con el número de caracteres en esa posición en el nombre de archivo. Además, no se pueden especificar signos de dólar en varias ubicaciones de un patrón de nombre de archivo, por ejemplo, {$$$}b{$$$}.log no coincide con abc.log. Dadas estas restricciones del signo de dólar, utilice patrones de nombre de archivo de expresión regular si hay un número indeterminado de caracteres en los nombres de archivo.
- El número total de signos de número y de interrogación que están especificados entre llaves es significativo. Debe coincidir con la parte del nombre de archivo con exactitud. Por ejemplo, el patrón AA{####} indica al proveedor de datos de archivo que busque archivos como AA0001. Lo nombres de archivo, como AA001 o AA00001, no se toman en consideración.
- El patrón de nombre de archivo exacto, las partes constantes y las numéricas deben coincidir con el nombre de archivo de forma exacta. Por ejemplo, el patrón AA{###} indica al proveedor de datos de archivo que compruebe el archivo AA101. Los nombres de archivo, como XAA101, AA222X y AA55555, no se toman en consideración.
- Utilice la cadena de patrón reservado {TIVOLILOGTIME} para sustituir la indicación de fecha y hora y el número de secuencia del archivo en un agente de Tivoli Monitoring o un archivo de registro de servidor. Esta cadena de patrón es útil cuando se realiza la supervisión automática de componentes de Tivoli Monitoring. Por ejemplo, si desea supervisar el último registro del servidor de supervisión en el directorio /opt/IBM/ITM/logs, puede especificar un patrón de nombre de archivo:

  ```
  /opt/IBM/ITM/logs/Host1_ms_{TIVOLILOGTIME}.log
  ```

  Si Host1_ms_452053c0-01.log, Host1_ms_451f11f4-01.log, Host1_ms_45205946-01.log y Host1_ms_451f11f4-02.log están presentes en el directorio /logs, el archivo Host1_ms_45205946-01.log se selecciona para supervisión.

Para especificar de forma precisa un nombre de archivo que consta de componentes de fecha (año, mes y día), utilice las letras mayúsculas Y, M y D. Estas letras deben especificarse entre llaves; de lo contrario se tratan como caracteres literales del nombre de archivo.

Vea los siguientes ejemplos:

{YYYYMMDD}.log
Especifica nombres de archivo como 20060930.log o 20061015.log.

{MMDDYY}.log
Especifica nombres de archivo como 101106.log o 110106.log.

{DDMMYYYY}.log
Especifica nombres de archivo como 01092006.log o 15082006.log.

{DDMMMYY}.log
Especifica nombres de archivo como 24Jan07 o 13Sep06.

{MM-DD-YY}.log
Especifica nombres de archivo como, por ejemplo, 11-02-06 o 04-29-07. El carácter separador (-) se ignora en el campo de fecha y no requiere un carácter de patrón de signo de interrogación para saltárselo.

MY{YYDDD}.log
Especifica nombres de archivo como MY06202.log, MY06010.log o MY04350.log.

Existen casos complejos, en los que un campo de datos se incluye dentro de un nombre de archivo más largo, y los patrones de fecha en los ejemplos anteriores no son suficientes. Para casos complejos, se crean patrones que combinen los signos de número y los interrogantes, y se siguen realizando comparaciones numéricas que seleccionen el archivo más actual para la supervisión. Por ejemplo, el

patrón ABC{?####?##?##?##?##?##?}XYZ.TXT se puede utilizar para nombres de archivo como ABC 2006-04-20 11_22_33 XYZ.TXT. En este ejemplo, solo está interesado en los dígitos marcados con #- y los signos de interrogación sirven de marcadores para ignorar otros caracteres del nombre de archivo.

El proveedor de datos de archivo comprueba periódicamente si hay archivos nuevos que coincidan con el patrón de archivo definido en la ubicación de vía de acceso de destino. Cuando se detecta un archivo nuevo que coincida con el patrón, el proveedor de datos de archivo cambia automáticamente la supervisión de la aplicación al nuevo archivo. El proveedor de datos de archivo busca el archivo que mejor coincida cuando:

- El proveedor de datos de archivo se inicia por primera vez.
- El archivo supervisado actualmente ya no existe debido a posibles renombres o supresiones.
- El contenido del archivo existente ha cambiado debido a posibles reescrituras.
- El intervalo de comprobación ha caducado. El intervalo predeterminado es 10 minutos. Puede cambiar el intervalo a un valor de intervalo más largo o más corto especificando la variable de entorno

```
KUMP_DP_FILE_SWITCH_CHECK_INTERVAL=número-de-segundos
```

Configuración de condiciones de excepción de SNMP

Descripción del archivo de configuración que utiliza el Proveedor de datos SNMP para devolver la información de interrupción en un formato legible más sencillo. El archivo también se utiliza para asignar categorías, gravedades, estatus e ID de origen a las condiciones de excepción.

También contiene las instrucciones para modificar el archivo predeterminado o sustituir su archivo de configuración.

Archivo de configuración de condiciones de excepción SNMP, `trapcnfg`

Durante el inicio, el Proveedor de datos SNMP lee un archivo de configuración denominado `trapcnfg`. Un objetivo de este archivo es traducir la información sobre condiciones de excepción SNMP a un formato más legible. Otro es asignar categorías, gravedades, estatus e ID de origen a condiciones de excepción específicas, ya que SNMP no define estas categorías.

Puede modificar el archivo `trapcnfg` para adaptarlo a las necesidades específicas de su sitio, añadiéndole nuevas definiciones de condición de excepción o Enterprise o cambiando las existentes. También puede utilizar su propio archivo de configuración.

Utilización del archivo `trapd.conf` de HP OpenView

El archivo `trapcnfg` es similar en formato, pero no idéntico, al archivo de configuración de condiciones de excepción de HP OpenView Network Node Manager `trapd.conf`. Puede copiar el archivo OpenView y volver a utilizar muchas de las sentencias de definición si es necesario.

Tipos de registros

`trapcnfg` contiene tres tipos de registros o bloques de registros:

comentarios
Los registros de comentario empiezan por un signo de número (#).

definiciones de Enterprise
Las definiciones de Enterprise se componen de dos señales delimitadas por espacios en blanco, donde la primera señal es un nombre y la segunda un identificador de objeto (OID) encerrado entre llaves ({ }).

definiciones de condición de excepción
Las definiciones de condición de excepción se componen de ocho señales delimitadas por espacios en blanco. Las definiciones de interrupción son registros de bloque ya que cada definición puede consistir en varios registros.

El primer tipo se explica por sí mismo. La Figura 87 en la página 1544 muestra ejemplos del segundo y tercer tipo.

El primer ejemplo en la Figura 87 en la página 1544 muestra un registrar de definición de empresa el cual define el ID de origen de la empresa 1.3.6.1.4.1.311.1.1.3.1.1 como Microsoft Windows NT.

El segundo ejemplo muestra un registro de definición de condición de excepción que define `trapName` `MSNTCOLD` como asociado al OID de empresa `1.3.6.1.4.1.311.1.1.3.1.1`, número de condición de excepción genérica 0 y número de condición de excepción específica 0. Tenga en cuenta que la gravedad se expresa en formato decimal, mientras que la categoría se expresa en formato de texto. Las gravedades se traducen a su forma textual antes de mostrarse. El siguiente registro del tipo bloque de registros 3 está en la descripción breve, que Agent Builder no utiliza. El Agent Builder utiliza la descripción detallada que se encuentra en los delimitadores SDESC y EDESC.

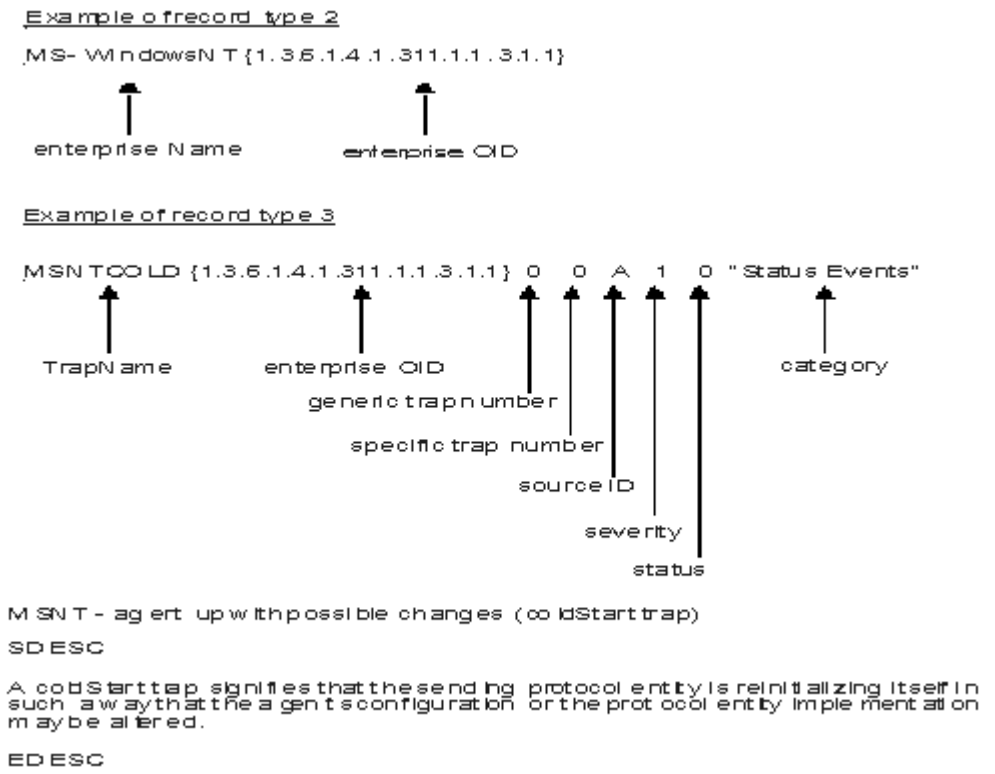


Figura 87. Ejemplos de registro de configuración tipos 2 y 3

Valores predeterminados para el archivo `trapcnfg`

Tablas que listan los valores predeterminados que soporta el Proveedor de datos SNMP.

Categorías soportadas

La Tabla 308 en la página 1544 muestra las categorías que soporta Agent Builder.

Tabla 308. Categorías soportadas por el Proveedor de datos de SNMP

Categoría	Representación textual
0	`Sucesos de umbral`

Tabla 308. Categorías soportadas por el Proveedor de datos de SNMP (continuación)	
Categoría	**Representación textual**
1	Sucesos de topología de red
2	Sucesos de error
3	Sucesos de estatus
4	Sucesos de configuración de nodo
5	Sucesos de alerta de aplicación
6	Todos los sucesos de categoría
7	Registrar sólo sucesos
8	Correlacionar sucesos
9	Ignorar sucesos

La Tabla 309 en la página 1545 lista las gravedades que soporta Agent Builder.

Tabla 309. Niveles de gravedad soportados por el Proveedor de datos de SNMP	
Gravedad	**Representación textual**
0	Borrar
1	Indeterminado
2	Aviso
3	Error leve
4	Crítico
5	Error grave

Estatus soportados

(Tabla 310 en la página 1545) muestra los estados que se definen en el archivo de configuración de Agent Builder.

Tabla 310. Estatus soportados por el Proveedor de datos de SNMP	
Estatus	**Representación textual**
0	Sin cambiar
1	Desconocido
2	Arriba
3	Marginal
4	Abajo
5	No gestionado
6	Reconocer
7	Usuario1
8	Usuario2

ID de origen soportados

La Tabla 311 en la página 1546 lista los ID de origen soportados por `trapcnfg`.

Tabla 311. IDs de fuente que soporta el Proveedor de datos de SNMP

ID de origen	Descripción
a	Aplicación
A	Agente
C	Xnmcollect
d	Demo
D	Recopilador de datos
E	Nvevents
I	Ipmap
L	LoadMIB
m	Shpmon
M	Topología IP
n	Relacionado con netmon
N	condiciones de excepción generadas por netmon
O	OSI SA
P	Condiciones de excepción no IP
r	Tralertd
s	Spappld
S	Agente de seguridad
t	Xnmtrap
T	Trapd
V	Relacionado con el proveedor
?	Desconocido

Consulta de mandatos de Actuación

Una visión general de los mandatos de actuación, referencias sobre los mandatos de actuación y descripciones de mandatos de actuación especiales.

Acerca de los mandatos de Actuación

Los mandatos de actuación se pueden incluir en un agente de supervisión de Agent Builder. Los mandatos de Actuación se pueden ejecutar desde el cliente de portal o se pueden incluir en una situación o en una política. Cuando se incluye en una situación, el mandato se ejecuta cuando la situación pasa a ser verdadera. Un mandato de actuación en una situación también se denomina automatización de reflejo. Cuando habilita un mandato de Actuación en una situación, automatiza una respuesta a condiciones del sistema. Por ejemplo, puede utilizar un mandato de actuación para enviar un mandato para reiniciar un proceso en el sistema gestionado. También puede utilizar un mandato de actuación para enviar un mensaje de texto a un teléfono móvil.

La automatización avanzada utiliza políticas para ejecutar acciones, planificar trabajo y automatizar tareas manuales. Una política consta de una serie de pasos automatizados, denominados actividades, que se conectan para crear un flujo de trabajo. Después de finalizar una actividad, Tivoli Enterprise Portal recibe información de código de retorno y la lógica de automatización avanzada responde con las actividades posteriores prescritas por dicha información de retorno.

Un mandato de actuación básico muestra el código de retorno de la operación en un recuadro de mensaje o un archivo de registro que se visualiza después de la finalización de la acción. Después de cerrar esta ventana, no hay más información disponible para esta acción.

Más información sobre los mandatos de Actuación

Para obtener más información sobre cómo trabajar con mandatos de actuación, consulte la publicación *Tivoli Enterprise Portal: Guía del usuario*.

Para obtener una lista y la descripción de los mandatos de actuación para este agente de supervisión, consulte "Mandatos de Actuación especiales" en la página 1547. Consulte también la información de dicha sección sobre cada mandato individual.

Mandatos de Actuación especiales

Un agente de supervisión de Agent Builder puede reconocer y realizar un proceso especial para un conjunto de mandatos de actuación:

- SSHEXEC

Para obtener más información sobre cómo crear estos mandatos e incluirlos en un proyecto de agente de supervisión de Agent Builder, consulte ("Creación de espacios de trabajo, mandatos de Actuación y situaciones" en la página 1408).

Acción SSHEXEC

Antes de empezar

Para obtener más información sobre los mandatos de actuación, consulte el "Consulta de mandatos de Actuación" en la página 1546.

Acerca de esta tarea

La acción SSHEXEC se reconoce para una aplicación supervisada que tenga al menos un grupo de atributos Script SSH. Indica que el mandato que sigue a la palabra clave SSHEXEC se inicia de forma remota en el sistema de destino SSH. El mandato se inicia con las credenciales y los privilegios del usuario que está configurado para que supervise el sistema de destino SSH. El mandato se ejecuta en el sistema remoto representado por el Nombre de sistema gestionado.

Procedimiento

Para incluir el mandato de Actuación en una situación o política de flujo de trabajo, utilice la siguiente sintaxis para el mandato del sistema:

```
SSHEXEC [Mandato]
```

Por ejemplo:

```
SSHEXEC [ls &vía_acceso]
```

Nota: Puede personalizar el mandato o partes del mandato durante la invocación de la actuación mediante la opción de argumentos de Actuación con el *Mandato*.

Nota: Si el *Mandato* incluye varios argumentos, entonces considere incluir los corchetes para habilitar la invocación del mandato de actuación con la interfaz de línea de mandatos **tacmd**.

Funciones de accesibilidad

Las características de accesibilidad ayudan a los usuarios con alguna discapacidad física como, por ejemplo movilidad restringida o visión limitada, a utilizar satisfactoriamente contenido de tecnologías de la información.

Funciones de accesibilidad

La interfaz basada en web de IBM Cloud Application Performance Management es la Consola de Cloud APM. La consola incluye las siguientes funciones de accesibilidad principales:

- Permite a los usuarios utilizar tecnologías de asistencia, tales como software de lector de pantalla y sintetizador de voz digital, para oír lo que se muestra en la pantalla. Consulte la documentación del producto de tecnología de asistencia para obtener información detallada sobre cómo utilizar dichas tecnologías con este producto.
- Permite a los usuarios utilizar funciones específicas o equivalentes utilizando sólo el teclado.
- Comunica toda la información independientemente del color.[1]

La Consola de Cloud APM utiliza el estándar W3C más reciente, WAI-ARIA 1.0 (http://www.w3.org/TR/wai-aria/), para asegurar conformidad con US Section 508 (http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards), y WCAG (Web Content Accessibility Guidelines) 2.0 . Para aprovechar las funciones de accesibilidad, utilice el release más reciente de su lector de pantalla junto con el navegador web más reciente soportados por este producto.

La documentación de producto en línea de la Consola de Cloud APM en el IBM Knowledge Center está habilitada para accesibilidad. Las funciones de accesibilidad de IBM Knowledge Center se describen en las Notas del release de IBM Knowledge Center .

Navegación mediante teclado

Este producto utiliza teclas de navegación estándar.

Información de la interfaz

La interfaz de usuario de web Consola de Cloud APM no se basa en hojas de estilo en cascada para representar el contenido de forma adecuada y para proporcionar una experiencia útil. Sin embargo, la documentación de producto sí se basa en hojas de estilo en cascada. IBM Knowledge Center proporciona una forma equivalente para que los usuarios con visión reducida utilicen sus ajustes de visualización personalizados, incluida la modalidad de contraste alto. Puede controlar el tamaño de letra utilizando los valores de navegador o de dispositivo.

La interfaz de usuario de web Consola de Cloud APM incluye puntos de referencia de navegación WAI-ARIA que puede utilizar para navegar rápidamente a áreas funcionales en la aplicación.

La interfaz de usuario Consola de Cloud APM no tiene contenido que se muestra intermitentemente de 2 a 55 veces por segundo.

Información de accesibilidad relacionada

Además de los sitios web de soporte y el centro de atención al cliente de IBM estándares, IBM ha establecido un servicio telefónico de teletipo para su uso por parte de clientes sordos o con dificultad de audición, para que puedan acceder a servicios de venta y de soporte:

servicio de teletipo 800-IBM-3383 (800-426-3383) (en Norteamérica)

[1] Las excepciones incluyen algunas de las páginas de **Configuración de agente** de la consola de Performance Management.

IBM y accesibilidad

Para obtener más información sobre el compromiso que tiene IBM con la accesibilidad, consulte IBM Accessibility (www.ibm.com/able).

Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en EE.UU. Este material puede estar disponible por parte de IBM en otros idiomas. Sin embargo, deberá poseer una copia del producto o de la versión del producto en ese idioma para poder acceder a él.

Puede que IBM no ofrezca en otros países los productos, servicios o funcionalidades tratados en este documento. Consulte al representante local de IBM para obtener información sobre los productos y servicios que se encuentran disponibles actualmente en su región. Las referencias a un producto, programa o servicio de IBM no pretenden afirmar ni dar a entender que sólo puede utilizarse ese producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o aplicaciones pendientes de patente que abarquen el tema descrito en este documento. La posesión de este documento no le otorga ninguna licencia relacionada con estas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Para realizar consultas sobre licencias relativas a la información del juego de caracteres de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe sus consultas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokio 103-8510, Japón

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, AUNQUE SIN LIMITARSE A, LAS GARANTÍAS DE NO CONTRAVENCIÓN, COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunas jurisdicciones no permiten la renuncia de garantías expresas o implícitas en ciertas transacciones, por lo que esta declaración podría no ser aplicable en su caso.

Esta información puede incluir imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras y/o cambios en los productos y/o los programas descritos en esta publicación, en cualquier momento y sin previo aviso.

Las referencias incluidas en esta información a sitios web no de IBM se proporcionan únicamente para su comodidad y no constituyen en modo alguno un aval de dichos sitios web. Los materiales de dichos sitios web no forman parte de los materiales para este producto de IBM y el uso de dichos sitios web corre a cuenta y riesgo del Cliente.

IBM puede utilizar o distribuir la información que usted le suministre del modo que IBM considere conveniente sin incurrir por ello en ninguna obligación para con usted.

Los propietarios de licencias de este programa que deseen tener información acerca de él con el objeto de habilitar: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido el presente) y (ii) el uso mutuo de la información que se ha intercambiado, deberán ponerse en contacto con:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones apropiados, que incluyen en algunos casos el pago de una cuota.

IBM proporciona el programa bajo licencia que se describe en este documento así como todo el material bajo licencia disponible para él mismo, según los términos del Acuerdo de cliente de IBM, del Acuerdo internacional de Programas bajo Licencia de IBM o de cualquier otro acuerdo equivalente entre ambas partes.

Los datos de rendimiento aquí comentados se presentan como derivados bajo condiciones de operación específicas. Los resultados reales pueden variar.

La información relativa a los productos no de IBM ha sido obtenida de los proveedores de dichos productos, sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado estos productos y no puede confirmar la exactitud del rendimiento, la compatibilidad o cualquier otra cuestión relacionada con los productos no de IBM. Las preguntas relativas a las prestaciones de los productos no de IBM deben dirigirse a los proveedores de dichos productos.

Las declaraciones relacionadas con la intención y orientación futura de IBM están sujetas a cambios o retiradas sin previo aviso y sólo representan objetivos y metas.

Esta información se proporciona únicamente para fines de planificación. La información contenida aquí puede cambiar antes de que los productos descritos pasen a estar disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen los nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con empresas o personas reales es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene ejemplos de programas de aplicaciones en lenguaje fuente que ilustran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo en cualquier formato sin necesidad de efectuar ningún pago a IBM, con el fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se ajusten a la interfaz de programación de aplicaciones para la plataforma operativa para la cual se han escrito los programas de aplicación. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por consiguiente, IBM no puede garantizar ni implicar la fiabilidad, servicio o funcionamiento de estos programas. Los programas de muestra se proporcionan "TAL CUAL", sin garantía de ninguna clase. IBM no es responsable de ningún daño resultante de la utilización de los programas de ejemplo por parte del usuario.

Todas las copias o partes de estos programas de ejemplo, o cualquier trabajo derivado, deben incluir un aviso de copyright
como se indica:
© (nombre de la empresa) (año).
Partes de este código se derivan de IBM Corp. Sample Programs.
© Copyright IBM Corp. 2014, 2015.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp. en varias jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM o de otras empresas. En Internet hay disponible una lista actualizada con las marcas registradas de IBM, en "Copyright and trademark information", en la dirección www.ibm.com/legal/copytrade.shtml.

Linux es una marca registrada de Linus Torvalds en EE.UU. o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle y/o sus afiliados.

Términos y condiciones de la documentación del producto

Los permisos para utilizar estas publicaciones se otorgan de acuerdo con los términos y condiciones siguientes.

Ámbito de aplicación

Estos términos y condiciones son adicionales a los términos de uso del sitio web de IBM.

Uso personal

Estas publicaciones se pueden reproducir para uso personal no comercial siempre que se conserven todos los avisos de propiedad. No puede distribuir, mostrar o realizar trabajo derivado de estas publicaciones, o de cualquier parte de las mismas, sin el consentimiento expreso de IBM.

Uso comercial

Puede reproducir, distribuir y mostrar estas publicaciones únicamente dentro de su empresa siempre que se preserven todos los avisos de la marca registrada. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Derechos

Salvo lo aquí permitido de forma expresa, no se conceden otros permisos, licencias o derechos, ni implícitos ni explícitos, para las publicaciones o cualquier información, datos software u otra propiedad intelectual que en ellas se incluya.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, a su discreción, el uso de las publicaciones sea perjudicial para sus intereses o que, según el parecer de IBM, no se sigan debidamente las instrucciones anteriores.

No puede descargar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO OFRECE NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO INFRACCIÓN E IDONEIDAD PARA UNA FINALIDAD DETERMINADA.

Declaración de privacidad en línea de IBM

Los productos de IBM Software, incluidas las soluciones de software como servicio, ("Ofertas de software") pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, para ayudar a mejorar la experiencia del usuario final, para adaptar las interacciones con el usuario final o

para otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta oferta de software utiliza cookies para recopilar información de identificación personal, la información específica sobre el uso de esta oferta de cookies se define más adelante en los párrafos siguientes.

En función de las configuraciones desplegadas, esta Oferta de software puede utilizar cookies de sesión que recopilan el nombre de cada usuario para gestionar sesiones, para la autenticación y para la configuración del inicio de sesión único. Estas cookies pueden inhabilitarse, pero si lo hace, es probable que se elimine la funcionalidad que habilitan.

Si las configuraciones desplegadas para esta Oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento legal sobre las leyes aplicables a dicha recopilación de datos, incluidos los requisitos de aviso y consentimiento.

Para obtener más información sobre el uso de varias tecnologías, incluidas las cookies, para dichos propósitos, consulte la Política de privacidad de IBM en http://www.ibm.com/privacy y la Declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details en la sección titulada "Cookies, balizas de web y otras tecnologías" y la "Declaración de privacidad de los productos de software de IBM software como servicio" en http://www.ibm.com/software/info/product-privacy.