Tivoli Application Dependency Discovery Manager
Versión 7.3

Guía del administrador

Tivoli Application Dependency Discovery Manager
Versión 7.3

Guía del administrador

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información que se incluye en el apartado "Avisos" en la página 285.

Aviso de la edición

Esta edición es aplicable a la versión 7, release 3 de IBM Tivoli Application Dependency Discovery Manager (número de producto 5724-N55) y todos los releases y modificaciones siguientes hasta que se indique de otro modo en las ediciones nuevas.

Contenido

Tablas

Acerca de este manual

El objetivo de esta versión del documento PDF es proporcionar los temas relacionados del Information Center en formato imprimible.

Convenios utilizados en este Information Center

En la documentación de IBM® Tivoli Application Dependency Discovery Manager (TADDM), se utilizan determinados convenios. Se utilizan para hacer referencia a las variables y las vías de acceso dependientes del sistema operativo, el directorio `COLLATION_HOME` y la ubicación del archivo `collation.properties`, a los que se hace referencia en la documentación de TADDM, incluido en los mensajes.

Vías de acceso y variables dependientes del sistema operativo

En este Information Center, se utilizan los convenios de UNIX para especificar las variables de entorno y la notación de directorios.

Cuando utilice la línea de mandatos de Windows, sustituya $*variable* por %*variable*% en las variables de entorno y las barras inclinadas (/) por barras inclinadas invertidas (\) en las vías de acceso a directorios.

Si utiliza la shell Bash en un sistema Windows, puede utilizar los convenios de UNIX.

Directorio `COLLATION_HOME`

El directorio raíz de TADDM también se conoce como el directorio `COLLATION_HOME`.

En sistemas operativos tales como AIX o Linux, la ubicación predeterminada para instalar TADDM es el directorio `/opt/IBM/taddm`. Por tanto, en este caso, el directorio `$COLLATION_HOME` es `/opt/IBM/taddm/dist`.

En sistemas operativos de Windows, la ubicación predeterminada para instalar TADDM es el directorio `c:\IBM\taddm`. Por lo tanto, en este caso, el directorio `%COLLATION_HOME%` es `c:\IBM\taddm\dist`.

Ubicación del archivo `collation.properties`

El archivo `collation.properties` contiene propiedades de servidor de TADDM e incluye comentarios de cada una de las propiedades. Está ubicado en el directorio `$COLLATION_HOME/etc`.

Términos y definiciones

Consulte la siguiente lista de términos y definiciones para conocer los conceptos más importantes de IBM Tivoli Application Dependency Discovery Manager (TADDM).

colección de accesos
Una colección que se utiliza para controlar el acceso a elementos de

configuración y a permisos para modificar elementos de configuración. Únicamente puede crear una colección de accesos cuando se ha habilitado la seguridad a nivel de datos.

descubrimiento asíncrono
En TADDM, la ejecución de un script de descubrimiento en un sistema de destino para descubrir sistemas a los que no se puede acceder directamente mediante el servidor de TADDM. Como el descubrimiento se realiza manualmente, y de forma independiente al descubrimiento con credenciales típico, éste se denomina "asíncrono".

aplicación empresarial
Una colección de componentes que proporciona una aplicación empresarial que puede utilizar de forma interna o externa o con otras aplicaciones industriales.

CI Consulte *elemento de configuración*.

recopilación
En TADDM, un grupo de elementos de configuración.

elemento de configuración (CI)
Componente de infraestructura de TI que está bajo el control de gestión de la configuración y por lo tanto está sujeto a control de cambios formal. Cada elemento de configuración de la base de datos de TADDM tiene un objeto persistente y un historial de cambios asociado a él. Ejemplos de un elemento de configuración son un sistema operativo, una interfaz de nivel 2 o un tamaño de agrupación de almacenamiento intermedio de base de datos.

Descubrimiento credencial
Exploración del sensor de TADDM que descubre información detallada sobre los siguientes elementos:

- Cada sistema operativo en el entorno de ejecución. Esta exploración también se conoce como descubrimiento de nivel 2 y necesita credenciales de sistema operativo.
- Infraestructura de aplicación, componentes de software desplegado, servidores físicos, dispositivos de red, sistemas virtuales y datos de host que se utilizan en el entorno de ejecución. Esta exploración también se conoce como descubrimiento de nivel 3 y necesita tanto las credenciales del sistema operativo como las credenciales de aplicación.

Descubrimiento de credenciales menores
Exploración del sensor TADDM que descubre información básica acerca de los sistemas informáticos activos en el entorno de ejecución. Esta exploración también se conoce como descubrimiento de nivel 1 y no necesita credenciales.

Portal de gestión de datos
Interfaz de usuario basada en web de TADDM para visualizar y manipular los datos en la base de datos de TADDM. Esta interfaz de usuario se puede aplicar a un despliegue de servidor de dominio, a un despliegue de servidor de sincronización y a cada servidor de almacenamiento de un despliegue de servidor en modalidad continua. La interfaz de usuario es muy parecida en todos los despliegues, aunque en un despliegue de servidor de sincronización, tiene menos funciones adicionales para añadir y sincronizar dominios.

hebra Worker de descubrimiento
En TADDM, una hebra que ejecuta sensores.

Consola de Discovery Management
Interfaz de usuario del cliente de TADDM para gestionar descubrimientos. Esta consola también se conoce como la Consola del producto. Es aplicable a un despliegue de servidor de dominio y a los Discovery Server en un despliegue de servidor continuo. La función de la consola es la misma para estos dos despliegues.

servidor de descubrimiento
Un servidor de TADDM que ejecuta sensores en un despliegue de servidor en modalidad continua pero que no tiene su propia base de datos.

dominio
En TADDM, un subconjunto lógico de infraestructura de una compañía u otra organización. Los dominios pueden definir límites organizativos, funcionales o geográficos.

servidor del dominio
Un servidor TADDM que ejecuta sensores en un despliegue de servidor de dominio tiene su propia base de datos.

despliegue de servidor de dominio
Despliegue de TADDM con un servidor de dominio. Un despliegue de servidor de dominio puede ser parte de un despliegue de servidor de sincronización.

En un despliegue de servidor de dominio, la siguiente propiedad de servidor de TADDM debe definirse con el siguiente valor:

```
com.collation.cmdbmode=domain
```

iniciar en contexto
El concepto de cambiar sin problemas de una interfaz de usuario de productos Tivoli a otra interfaz de usuarios de productos Tivoli (en una consola diferente o en la misma interfaz de consola o de portal) con un inicio de sesión único y con la interfaz de usuario de destino en el punto adecuado para que los usuarios puedan continuar con sus tareas.

Descubrimiento de nivel 1
Exploración del sensor TADDM que descubre información básica acerca de los sistemas informáticos activos en el entorno de ejecución. Esta exploración también se conoce como descubrimiento sin credenciales y, como su propio nombre indica, no necesita credenciales. Utiliza el sensor Stack Scan y el sensor IBM® Tivoli® Monitoring Scope. El descubrimiento de nivel 1 es muy superficial. Recoge solo el nombre de host, el nombre del sistema operativo, la dirección IP, el nombre de dominio completo y la dirección Media Access Control (MAC) de cada interfaz descubierta. Además, el descubrimiento de dirección MAC se limita a Linux en los sistemas System z® y Windows. El descubrimiento de nivel 1 no descubre subredes. Para cada interfaz IP descubierta que no pertenezca a ninguna subred existente hallada durante el descubrimiento de nivel 2 o de nivel 3, se crean subredes nuevas basadas en el valor de la propiedad `com.collation.IpNetworkAssignmentAgent.defaultNetmask` del archivo `collation.properties`.

Descubrimiento de nivel 2
Exploración del sensor TADDM que descubre información detallada acerca de cada sistema operativo en el entorno de ejecución. Esta exploración también se conoce como descubrimiento con credenciales y necesita credenciales de sistema operativo. El descubrimiento de nivel 2 recopila los nombres de la aplicación y los nombres del sistema operativo, así como los números de puertos asociados con cada aplicación en ejecución. Si una

aplicación ha establecido una conexión TCP/IP con otra aplicación, se captura esta información como una dependencia.

Descubrimiento de nivel 3
Exploración del sensor de TADDM que descubre información detallada sobre la infraestructura de la aplicación, los componentes del software desplegados, los servidores físicos, los dispositivos de red, los sistemas virtuales y los datos de host utilizados en el entorno de ejecución. Esta exploración también se conoce como descubrimiento con credenciales y necesita tanto las credenciales del sistema operativo como las credenciales de aplicación.

tenencia múltiple
En TADDM, la utilización por parte de un proveedor de servicio o de tecnologías de la información de una instalación de TADDM para descubrir varios entornos de clientes. Además, el proveedor de servicios o proveedor de TI puede ver los datos de todos los entornos de cliente, pero dentro de cada entorno de cliente, y sólo los datos específicos del cliente respectivo se pueden visualizar en la interfaz de usuario o en los informes de dicho entorno de cliente.

Consola del producto
Consulte *consola de Discovery Management*.

descubrimiento basado en un script
En TADDM, la utilización, en un descubrimiento credencial, de los mismos scripts de sensor proporciona apoyo al descubrimiento asíncrono.

SE Consulte *equivalente de servidor*.

equivalente de servidor (SE)
Unidad representativa de infraestructura de TI definida como un sistema informático (con configuraciones estándar, sistemas operativos, interfaces de red e interfaces de almacenamiento) con software de servidor instalado (como una base de datos, un servidor web o un servidor de aplicaciones). El concepto de un equivalente de servidor también incluye la red, el almacenamiento y otros subsistemas que proporcionan servicios para el funcionamiento óptimo del servidor. Un servidor equivalente depende del sistema operativo:

Sistema operativo	Número aproximado de CI
Windows	500
AIX	1000
Linux	1000
HP-UX	500
Dispositivos de red	1000

servidor de almacenamiento
Servidor TADDM que procesa los datos de descubrimiento recibidos de los Discovery Servers y los almacena en la base de datos. El servidor de almacenamiento primario coordina tanto los servidores de descubrimiento como todos los otros servidores y funciona como servidor de almacenamiento. Todos los servidores de almacenamiento que no son el servidor primario se llaman servidores de almacenamiento secundario.

despliegue del servidor de modalidad continua
Despliegue de TADDM con un servidor de almacenamiento primario y al menos un servidor de descubrimiento. Este tipo de despliegue también

puede incluir uno o más servidores de almacenamiento secundarios opcionales. El servidor de almacenamiento primario y secundario comparten la base de datos. Los servidores de descubrimiento no tienen base de datos.

En este tipo de despliegue, los datos de descubrimiento fluyen en paralelo desde los servidores de descubrimiento múltiples a una base de datos de TADDM.

En un despliegue de servidor en modalidad continua, la propiedad del siguiente servidor de TADDM debe enviarse a uno de los siguientes valores:

- `com.collation.taddm.mode=DiscoveryServer`
- `com.collation.taddm.mode=StorageServer`

Para todos los servidores excepto el servidor de almacenamiento primario, las siguientes propiedades (para el nombre de host y el número de puerto del servidor de almacenamiento primario) también deben definirse:

- `com.collation.PrimaryStorageServer.host`
- `com.collation.PrimaryStorageServer.port`

Si la propiedad com.collation.taddm.mode está definida, la propiedad com.collation.cmdbmode debe definirse o comentarse.

servidor de sincronización
Un servidor de TADDM que sincroniza los datos de descubrimiento desde todos los servidores de dominio en la empresa tiene su propia base de datos. Este servidor no descubre los datos directamente.

despliegue del servidor de sincronización
Un despliegue de TADDM con un servidor de sincronización y dos o más despliegues de servidor de dominio, cada uno de los cuales tiene su propia base de datos local.

En este tipo de despliegue, el servidor de sincronización copia los datos de descubrimiento desde servidores de dominio múltiples, un dominio cada vez en procesos de sincronización de lotes.

En un despliegue de servidor de sincronización, la siguiente propiedad del servidor de TADDM debe definirse al siguiente valor:

`com.collation.cmdbmode=enterprise`

Este tipo de despliegue está obsoleto. Por tanto, en un nuevo despliegue de TADDM donde se necesita más de un servidor, utilice el despliegue de servidor en modalidad continua. Un servidor de sincronización puede convertirse en un servidor de almacenamiento primario para el despliegue del servidor en modalidad continua.

Base de datos de TADDM
En TADDM, la base de datos donde se almacenan los datos de configuración, las dependencias y el historial de cambios.

Cada servidor de TADDM, excepto los servidores de descubrimiento y los servidores de almacenamiento secundario, tiene su propia base de datos. Los servidores de descubrimiento no tienen base de datos. Los servidores de almacenamiento comparten la base de datos del servidor de almacenamiento primario.

servidor de TADDM
Un término genérico que puede representar cualquiera de los siguientes términos:

- servidor de dominio en un despliegue de servidor de dominio
- servidor de sincronización en un despliegue de servidor de sincronización
- servidor de descubrimiento en un despliegue de servidor en modalidad continua
- servidor de almacenamiento (incluido el servidor de almacenamiento primario) en un despliegue de servidor en modalidad continua

sistema de destino
En el proceso de descubrimiento de TADDM, el sistema que se va a descubrir.

Descubrimiento de utilización
Exploración del sensor de TADDM que descubre información de utilización para el sistema host. Un descubrimiento de utilización requiere credenciales del sistema operativo.

Administración

Visión general de TADDM

IBM Tivoli Application Dependency Discovery Manager (TADDM) es una herramienta de gestión de la configuración que ayuda al persona de operaciones de TI a asegurar y mejorar la disponibilidad de la aplicación en entornos de aplicación. TADDM proporciona los detalles de los elementos de configuración mediante el descubrimiento automatizado y sin agente de activos y sus dependencias de aplicación, además incluye tecnología de biblioteca de descubrimientos para ayudar a la optimización de datos desde otras fuentes.

TADDM proporciona al personal operativo una vista de arriba a abajo de las aplicaciones, de modo que puedan entender rápidamente la estructura, el estado, la configuración y el historial de cambios de las aplicaciones críticas de negocio. Cuando se produce el problema de rendimiento y disponibilidad, esta vista ayuda al personal a aislar los problemas inmediatamente y a planificar más eficazmente el cambio de aplicaciones sin molestias. Se crea y se mantiene la base de datos de TADDM, una base de datos de gestión de configuración, que no requiere modelado de infraestructura personalizado. TADDM también proporciona mapas completos de dependencia entre niveles, vistas de topología, rastreo de cambios, propagación de sucesos e informes y analíticas detalladas.

TADDM depende del descubrimiento de información, que se realiza mediante sensores que se despliegan como parte del producto de TADDM. Los datos resultantes del proceso de descubrimiento se utilizan para crear mapas de dependencia entre niveles que enlazan topologías físicas y lógicas. Este directorio jerárquico representa el entorno de ejecución completo.

Los siguientes pasos son un resumen de alto nivel de lo que TADDM hace:

1. Los sensores determinan y recopilan la identidad, los atributos y valores de cada aplicación, sistema y componente de red.
2. Los datos de configuración, las dependencias y el historial de cambios se almacenan en la base de datos de TADDM y las topologías se almacenan en el servidor de TADDM. Cuando se descubren los elementos de configuración, se almacenan en la base de datos de TADDM desde los siguientes orígenes:
   - Sensores
   - Los libros de la biblioteca de descubrimiento, conocidos también como libros IdML (Identity Development Markup Language), que se generan mediante sistemas de software de gestión externos
   - API
3. Los datos descubiertos se visualizan como topologías de aplicaciones de tiempo de ejecución y entre niveles en la interfaz de usuario de TADDM. Los descubrimientos subsiguientes actualizan la topología. Además, TADDM mantiene un historial de cambios de la configuración y las dependencias de la infraestructura.
4. TADDM genera informes y vistas topológicas adicionales de la información almacenada en la base de datos de TADDM.

Entidades que descubre TADDM

Tabla 1 lista y describe las entidades que TADDM descubre en el entorno.

Tabla 1. Entidades descritas con descripciones

Entidad	Descripción
Nivel de red	Los siguientes dispositivos se descubren con los valores de parámetro de MIB2 (RFC 1213) para cada dispositivo: • Direccionadores • Conmutadores • Equilibradores de carga • Cortafuegos • Dispositivos de IP genéricos
Nivel del sistema	Los siguientes dispositivos se descubren en el nivel de sistema: • Hosts y discos del servidor • Interfaces IP de host • Servidores de la bases de datos • Equilibradores de carga o clústeres
Nivel de aplicación	Los siguientes componentes se descubren en el nivel de aplicación. Además, para cada componente (excepto para los procesos genéricos) se descubre información sobre la versión, archivos y propiedades de configuración, información de host y extensiones específicas del proveedor. • Servidores personalizados, basados en plantillas personalizadas que se diseñan • Servidores y configuraciones de aplicaciones Java EE • Componentes y módulos de Java EE y Java SE • Componentes del servidor web • Módulos web, archivos de configuración y directorios de instalación • Procesos de JVM genéricos • Bases de datos
Servicios de infraestructura	Se descubren los servicios de infraestructura del sistema que soportan el entorno de la aplicación y se descubren la estructura de dependencia entre estos componentes de servicio y los componentes de la aplicación. Los siguientes componentes se encuentran en el servicio de infraestructura: • Servicios DNS y NFS • LDAP
Estructura de relaciones	Además del descubrimiento de componentes, se descubre la conectividad lógica y física de los niveles de red, sistema y aplicación en el siguiente nivel de cada nivel: • Conectividad de IP de capa 3 • Conectividad de capa 2 • Dependencias de tiempo de ejecución del componente de la aplicación • Dependencias del servicio de infraestructura

Se descubren configuraciones e interdependencias en las siguientes entidades:

- Componentes de la aplicación, como servidores web, servidores de aplicación y bases de datos
- Componentes del sistema, como hosts, sistemas operativos, equilibradores de carga y servidores de bases de datos
- Componentes de red, como direccionadores, conmutadores y cortafuegos
- Servicios de infraestructura, como servicios de DNS y LDAP

Nota: El uso de direcciones IP virtuales o varios controladores de interfaz de red puede hacer que TADDM notifique resultados incorrectos. Al planificar un descubrimiento, tenga en cuenta la infraestructura de red.

Visión general del proceso de descubrimiento

El descubrimiento es un proceso multinivel que recopila información de configuración sobre la infraestructura completa de la aplicación, incluyendo la identificación de componentes de software desplegados, servidores físicos, dispositivos de red, sistemas virtuales y datos de host utilizados en el entorno de ejecución. El descubrimiento se realiza mediante sensores que forman parte del producto TADDM.

El trabajo del sensor es descubrir elementos de configuración, crear objetos de modelo y hacer que estos objetos de modelo permanezcan en la base de datos de TADDM. Los sensores utilizan protocolos que son específicos de los recursos que están destinados a descubrir. Algunos ejemplos son los siguientes protocolos:

- Cisco Discovery Protocol (CDP)
- Java™ Management Extensions (JMX)
- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP)
- Structured Query Language (SQL)

Cuando es posible, se utiliza una conexión segura entre el servidor de TADDM y los sistemas de destino.

TADDM no ejecuta descubrimientos sobre redes IPv6, pero los atributos de IPv6 los descubren los descubrimientos que se ejecutan en redes IPv4.

Sensores

TADDM proporciona un abanico de sensores especializados para el descubrimiento de casi todos los componentes en el centro de datos típico, en el software de la aplicación, host y los niveles de red. También se pueden desarrollar sensores personalizados para componentes exclusivos. Los sensores se encuentran en el servidor de TADDM y recopilan atributos y dependencias de configuración.

Los sensores no son intrusivos, lo que significa que se ejecutan en el servidor de TADDM en lugar de en una estación de trabajo del cliente. Por lo tanto, mediante el uso de TADDM, puede recopilar información relacionada con el descubrimiento sin incurrir en los costes de instalación y mantenimiento locales del agente en cada estación de trabajo de cada cliente que desee descubrir.

Como los sensores utilizan conexiones de red seguras, las credenciales de acceso cifradas y los programas de utilidad nativos de host, son seguros y proporcionan el mismo nivel de adquisición de datos que tiene cuando utiliza software que está ubicado en la estación de trabajo del cliente.

Un sensor tiene los siguientes tres aspectos configurables:

Ámbito
Ámbito de descubrimiento es normalmente un rango de IP válido, una subred o una dirección específica. Define el límite para el descubrimiento.

Lista de acceso
Lista de acceso es una colección de credenciales, como nombres de usuario, contraseñas y series de comunidad del protocolo simple de gestión de red (SNMP), que el sensor utiliza al acceder a los elementos de configuración en la infraestructura de la aplicación. Debe configurar la lista de acceso para los elementos de configuración que desee descubrir.

Planificación
El descubrimiento se puede ejecutar a demanda, por planificación o puede estar motivado por sucesos desencadenantes externos. La planificación identifica si los sensores se ejecutan a demanda o por planificación.

Cómo un sensor descubre los elementos de configuración:

En estos pasos se describe cómo un sensor descubre los elementos de configuración en su entorno.

1. Para identificar los dispositivos de IP activos en el ámbito especificado, el sensor intenta establecer una conexión de protocolo de control de transmisiones (TCP) en varios puertos (como el 22, 23 y el 135) con el fin de detectar una respuesta. Cualquier respuesta es suficiente para informar al sensor de que el dispositivo existe.
2. El sensor intenta conectarse al dispositivo de IP en varios puertos (como el 22 y el 135) para determinar la tecnología que va a utilizar para descubrir el host.
3. Si un puerto que utiliza un protocolo de Secure Shell (SSH) está abierto, el sensor intenta establecer una conexión de SSH mediante credenciales de la lista de acceso. A continuación, el sensor intenta acceder a las entradas de la lista de acceso de tipo **sistema informático** o **sistema informático Windows** hasta que una entrada funciona o el sensor llega al final de la lista de acceso sin éxito.
4. Si un puerto de Windows Management Instrumentation (WMI) está abierto, se establece una conexión de SSH con un sistema informático de pasarela (si se encuentra uno para el sistema de destino). A continuación, el sensor intenta acceder a las entradas de la lista de acceso de tipo**sistema informático Windows** hasta que una entrada funciona o el sensor llega al final de la lista de acceso sin éxito.
5. Si no se puede establecer una sesión, se ejecuta un sensor de protocolo simple de gestión de red (SNMP). Si se establece una sesión, se ejecuta un sensor para el sistema informático.
6. Un sensor del sistema informático intenta determinar el tipo de sistema operativo que está instalado.
7. TADDM ejecuta un sensor que es específico del sistema operativo y que lo descubre en mayor detalles.
8. Durante el descubrimiento en mayor detalle del sistema operativo, basado en criterios específicos (como el número de puerto y el nombre del proceso), TADDM ejecuta sensores específicos del software para descubrir los detalles de la aplicación.

Iniciación de un sensor de aplicación:

Esta información describe cómo se inicia un sensor de una aplicación.

GenericServerSensor ejecuta los siguientes mandatos:

En los sistemas operativos Linux, Solaris, AIX, y Linux on System z

- **lsof -nP -i** para obtener la información del puerto
- **ps axww** para obtener la información de la línea de mandatos

En sistemas operativos Windows

- **netstat.exe -nao** para obtener la información del puerto
- **wmic process list** para obtener la información de la línea de mandatos

El ID de proceso (PID) se utiliza para fusionar la salida. A continuación, el buscador de coincidencias de plantillas opera en los datos fusionados. Cuando el nivel de registro se define en DEBUG en el archivo `collation.properties`, la salida de estos mandatos se ubica en los siguientes registro:

- `GenericServerSensor.log`
- `DiscoverManager.log`

Los datos fusionados deben coincidir con los criterios definidos en la plantilla del sensor. Puede encontrar los criterios de la plantilla que inician un sensor en la siguiente definición de plantilla de muestra para el sensor DB2.

Ejecute el siguiente mandato (una redirección a un archivo es útil), sustituyendo *<username>* y *<password>* por un nombre de usuario válido y una contraseña asociada (por ejemplo, `...dist/sdk/bin/api.sh -u administrator -p collation find --depth=5 AppServerTemplate`):

```
...dist/sdk/bin/api.sh -u <nombre_usuario> -p <contraseña> find --depth=5 AppServerTemplate
```

El mandato anterior produce una salida de XML que es la definición de la plantilla. En la definición de la plantilla, si el valor para el elemento `<order>` es inferior a 0, la plantilla es para un sensor. Si el valor para el elemento `<order>` es superior a 0, la plantilla es para un servidor personalizado. La coincidencia se produce comenzando por el valor inferior para el elemento `<order>` de modo que los sensores obtienen mayor prioridad de coincidencia que los servidores personalizados.

La definición de la plantilla de muestra es para el sensor DB2. Observe dos elementos `<operand1>`, uno con el valor `db2tcpcm` y otro, con el valor `db2agent`. El valor del elemento `<boolExp>` indica si deben existir ambos valores del `<operand1>` o solo uno. Un valor de `1` para el elemento `<boolExp>` indica el operador lógico OR, que significa que sólo uno de los valores `<operand1>` debe existir. Un valor de `0` para el elemento `<boolExp>` indica el operador lógico AND, que significa que ambos valores de `<operand1>` deben existir.

```
<Template array="18" guid="C1A992327AFF33409C41D5C71046DBB9"
lastModified="1177555771479"
xsi:type="coll:com.collation.platform.model.discovery.template.AppServerTemplate">
   <displayName>DB2</displayName>
   <name>DB2</name>
   <type>DatabaseServer</type>
   <internal>true</internal>
   <filterSet guid="B599AED918F436C99FDA0E8EDA578F02"
   lastModified="1177555771475"
   parent="C1A992327AFF33409C41D5C71046DBB9"
   xsi:type="coll:com.collation.platform.model.discovery.template.FilterSet">
```

```
      <displayName>DB2</displayName>
      <filterList array="1"
      guid="BBE4D351653B37E38BFFD2DEBD532EE8"
      lastModified="1177555771476"
      parent="B599AED918F436C99FDA0E8EDA578F02"
      xsi:type="coll:com.collation.platform.model.discovery.template.Filter">
         <displayName>unknown</displayName>
         <operand1>db2tcpcm</operand1>
         <operator>contains</operator>
         <part>Program Name</part>
      </filterList>
      <filterList array="2"
      guid="63816C902B0A317F8C3B24C7A1EEBC17"
      lastModified="1177555771471"
      parent="B599AED918F436C99FDA0E8EDA578F02"
      xsi:type="coll:com.collation.platform.model.discovery.template.Filter">
         <displayName>unknown</displayName>
         <operand1>db2agent</operand1>
         <operator>contains</operator>
         <part>Program Name</part>
      </filterList>
      <boolExp>1</boolExp>
   </filterSet>
   <index>0</index>
   <order>-10</order>
   <enabled>true</enabled>
   <action>1</action>
   <source>0</source>
   <seedClass>com.collation.discover.seed.app.db.db2.Db2Seed</seedClass>
</Template>
```

Niveles de descubrimiento

TADDM proporciona cuatro niveles de descubrimiento: descubrimiento de nivel 1, descubrimiento de nivel 2, descubrimiento de nivel 3 y descubrimiento de utilización.

Descubrimiento de nivel 1

Exploración del sensor TADDM que descubre información básica acerca de los sistemas informáticos activos en el entorno de ejecución. Esta exploración también se conoce como descubrimiento *sin credenciales*, ya que no requiere credenciales. Utiliza el sensor Stack Scan y el sensor IBM Tivoli Monitoring Scope.

El descubrimiento de nivel 1 es muy superficial. Éste sólo recopila el nombre de host, el nombre del sistema operativo, la dirección IP, el nombre de dominio totalmente cualificado y la dirección del control de acceso al medio (MAC) de cada interfaz que se haya descubierto. Además, el descubrimiento de la dirección de control de acceso a soportes está limitado a los sistemas Linux en System z y Windows.

El descubrimiento de nivel 1 no descubre subredes. Para cualquier interfaz de IP descubierta que no pertenezca a ninguna subred existente descubierta durante el descubrimiento de nivel 2 y nivel 3, se crean nuevas subredes basadas en el valor de la propiedad com.collation.IpNetworkAssignmentAgent.defaultNetmask en el archivo `collation.properties`.

Descubrimiento de nivel 2

Exploración del sensor TADDM que descubre información detallada acerca de cada sistema operativo en el entorno de ejecución. Esta exploración también se conoce como descubrimiento *con credenciales*, ya que requiere credenciales del sistema operativo.

El descubrimiento de nivel 2 recopila los nombres de la aplicación y los nombres del sistema operativo, así como los números de puertos asociados con cada aplicación en ejecución. Si una aplicación ha establecido una conexión TCP/IP con otra aplicación, se captura esta información como una dependencia.

Descubrimiento de nivel 3
Exploración del sensor de TADDM que descubre información detallada sobre la infraestructura de la aplicación, los componentes del software desplegados, los servidores físicos, los dispositivos de red, los sistemas virtuales y los datos de host utilizados en el entorno de ejecución. Esta exploración también se conoce como descubrimiento *con credenciales* y requiere credenciales del sistema operativo y credenciales de la aplicación.

Descubrimiento de utilización
Exploración del sensor de TADDM que descubre información de utilización para el sistema de host. Un descubrimiento de utilización requiere credenciales del sistema operativo.

Los descubrimientos de nivel 2 y 3 capturan información más detallada que los descubrimientos de nivel 1. Si los objetos creados durante un descubrimiento de nivel 2 o nivel 3 coinciden con los objetos creados anteriormente por un descubrimiento de nivel 1, los objetos de nivel 1 se sustituyen por los objetos recién creados que, a su vez, hace que los identificadores exclusivos globales de los objetos cambien. Por lo tanto, y en general, los datos de nivel 1 no deben utilizarse para la integración con otros productos.

Perfiles de descubrimiento

Para ejecutar un descubrimiento, debe especificar un perfil de descubrimiento, que define un conjunto de opciones para el descubrimiento. Mediante los perfiles de descubrimiento, puede configurar sensores individuales, gestionar varias configuraciones del mismo sensor, seleccionar la configuración adecuada en función de una serie de criterios y gestionar conjuntos de configuración de sensores diferentes para que se apliquen en una sola ejecución del descubrimiento.

Al seleccionar el perfil de descubrimiento apropiado, puede controlar la profundidad del descubrimiento o el nivel de éste.

De forma predeterminada, TADDM proporciona cuatro perfiles de descubrimiento. Tres son para los tres niveles de descubrimiento que puede elegir (nivel 1, nivel 2 o nivel 3), según desee llevar a cabo un descubrimiento con credenciales o sin credenciales. El perfil restante es para un descubrimiento de utilización.

Si no se especifica ningún perfil, el perfil de descubrimiento de nivel 3 se utiliza de forma predeterminada, aunque puede cambiar el perfil predeterminado en la consola de Discovery Management.

Para obtener información adicional sobre los perfiles de descubrimiento, consulte *A Flexible Approach to Discovery* (un enfoque flexible al descubrimiento) en la wiki de TADDM en https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/A%20Flexible%20Approach%20to%20Discovery.

Habilitación e inhabilitación de sensores

Puede inhabilitar globalmente un sensor aunque un perfil haya habilitado el sensor. También puede habilitar globalmente un sensor y permitir que el valor funcione en el perfil.

Por ejemplo, si un sensor está habilitado globalmente y está habilitado en el perfil, el sensor se ejecuta. Si el sensor está habilitado globalmente, pero inhabilitado en el perfil, el sensor no se ejecuta cuando se selecciona el perfil mencionado anteriormente para su descubrimiento.

Para que la habilitación e inhabilitación globales funcionen para los sensores con un directorio `osgi` (`$COLLATION_HOME/osgi/plugins`), debe cambiar el mandato **`AgentConfigurations`** en el directorio `osgi`.

Por ejemplo, para Db2Sensor, busque los siguientes directorios:

- `$COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.app.db.db2_x.x.x/Db2Sensor.xml`
- `$COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.app.db.db2windows_x.x.x/Db2WindowsSensor.xml`

donde *x.x.x* es la versión del plug-in del sensor, por ejemplo `7.3`.

Al editar los archivos XML, para habilitar el sensor, establezca la habilitación en `true`. Para inhabilitar el sensor, establezca la habilitación en `false`.

Para los sensores que no utilicen el directorio `osgi/plugins`, la información de configuración se almacena en e l archivo de configuración del sensor que está en el directorio `etc/discover-sensors`.

Descubrimiento asíncrono y basado en script

En el descubrimiento asíncrono y en el descubrimiento basado en scripts, en lugar de ejecutar mandatos individuales, los sensores proporcionan un script de descubrimiento, que ejecutan en el sistema de destino.

No todos los sensores soportan el descubrimiento asíncrono y el descubrimiento basado en script. Sólo los sensores que proporcionan script de descubrimiento soportan estos tipos de descubrimiento.

Para obtener información sobre los sensores que admiten el descubrimiento asíncrono y el descubrimiento basado en scripts, consulte el tema *Sensores que admiten el descubrimiento asíncrono y el descubrimiento basado en scripts* de la *Referencia de sensores* de TADDM.

Algunas diferencias respecto a un descubrimiento no basado en script

El descubrimiento asíncrono y el descubrimiento basado en script se diferencian del descubrimiento no basado en script en los siguientes aspectos importantes:

- En comparación con los resultados de descubrimientos de un descubrimiento de nivel 2 o 3 no basado en script, un descubrimiento que es el resultado de un descubrimiento asíncrono o de un descubrimiento basado en script, puede no resultar tan completo. La mayoría de los sensores descubren un mayor número de objetos, atributos y relaciones en un descubrimiento no basado en script que en un descubrimiento asíncrono o basado en script.
- En el descubrimiento asíncrono o basado en script, los sensores de la aplicación sólo se inician una vez en cada sistema determinado. Sin embargo, si la

aplicación está a la escucha en más de un puerto, se descubre cada instancia de aplicación.
En un descubrimiento no basado en script, se inicia un sensor de la aplicación para cada instancia de la aplicación.

Descubrimiento asíncrono:

Puede ejecutar el descubrimiento asíncrono para descubrir sistemas a los que el servidor de TADDM no puede acceder directamente. Se incluyen los sistemas que están en ubicaciones seguras (por ejemplo, sistemas a los que no se puede acceder a través de red), sistemas en los que no se ejecuta Secure Shell (SSH) y sistemas con información confidencial para los que no se pueden obtener credenciales.

En el descubrimiento asíncrono, los usuarios ejecutan un script de descubrimiento en un sistema de destino. El script de descubrimiento contiene un script principal y varios scripts del sensor. Cada script de sensor proporciona una capacidad de descubrimiento similar a una función que efectúa el sensor al ejecutarse en un descubrimiento típico.

La salida del script de descubrimiento es un archivo de archivado que contiene los resultados del descubrimiento. Debe copiar este archivo al servidor de TADDM. Durante el descubrimiento de TADDM, los sensores de TADDM procesan los resultados del descubrimiento desde un archivo de archivado (en lugar de ejecutar mandatos).

Como el descubrimiento se lleva a cabo manualmente y de forma independiente al descubrimiento típico con credenciales, éste se denomina “asíncrono”.

Para ejecutar un descubrimiento asíncrono se necesita el sensor del descubrimiento asíncrono. Para obtener más información, consulte TADDM*Referencia al sensor*.

Para obtener información sobre cómo configurar los sensores para ejecutar el descubrimiento asíncrono, consulte “Configuración del descubrimiento asíncrono” en la página 108.

Descubrimiento basado en script:

En los descubrimientos basados en scripts puede utilizar un script de descubrimiento en un descubrimiento típico, en el que se solicitan las credenciales. En este tipo de descubrimiento se utilizan los mismos scripts de sensor que en el descubrimiento asíncrono.

En un descubrimiento basado en script, un sensor no ejecuta mandatos individuales. En su lugar, el script del sensor se ejecuta en el sistema de destino. Puede que no sean necesarias las credenciales específicas de la aplicación.

Por ejemplo, para descubrir la aplicación IBM WebSphere en un descubrimiento típico, debe crear una entrada de lista de acceso con credenciales para la aplicación WebSphere si se ha habilitado la seguridad. Sin embargo, mediante el uso del descubrimiento basado en script, no es necesaria la entrada de lista de acceso de WebSphere. El descubrimiento basado en script también elimina el uso de los protocolos específicos de la aplicación como Java Management Extensions (JMX), que puede ampliar el descubrimiento de la aplicación a través IBM Tivoli Monitoring.

Para obtener información sobre cómo configurar los sensores para ejecutar el descubrimiento basado en scripts, consulte “Configuración del descubrimiento basado en script” en la página 112.

Descubrimiento simultáneo

Puede ejecutar más de un descubrimiento al mismo tiempo, en lo que se llama *descubrimiento simultáneo*. Por ejemplo, ya que un descubrimiento grande puede tardar varias horas en completarse, es posible que desee iniciar descubrimientos más pequeños antes de que finalice el descubrimiento más grande. Antes de ejecutar cualquier descubrimiento simultáneo, debe configurarlo correctamente.

Puede ejecutar un descubrimiento simultáneo utilizando un perfil de descubrimiento diferente al utilizado para iniciar el primer descubrimiento.

Para gestionar descubrimiento simultáneos, utilice la consola de Discovery Management o el script `api.sh`. Para obtener más información sobre el uso del script `api.sh`, consulte el tema *API de interfaz de línea de mandatos* en la *Guía del desarrollador del SDK* de TADDM.

Puede ejecutar descubrimientos simultáneos en el mismo destino. Si uno o más descubrimientos supervisan algunas de las mismas direcciones IP, cada descubrimiento funciona independientemente.

Si se cambia la contraseña mientras se está ejecutando un descubrimiento, y se inicia un descubrimiento simultáneo, los sensores de dicho descubrimiento simultáneo utilizarán inmediatamente las nuevas credenciales, presuponiendo que dichos sensores no se han iniciado antes del cambio de contraseña.

TADDM no da soporte al descubrimiento simultáneo con una lista de accesos basada en perfiles.

Si los cambios se realizan en la plantilla del servidor personalizado mientras se ejecuta un servidor de descubrimiento, cualquier descubrimiento no simultáneo que se inicia sigue utilizando la versión existente de la plantilla del servidor personalizado. El siguiente descubrimiento separado, no simultáneo que se inicie utilizará la nueva versión de la plantilla del servidor personalizado.

Determinación del nombre de dominio completo (FQDN) visualizado

Es posible configurar un método preferido para la determinación del nombre de dominio completo (FQDN) para cada sistema descubierto.

Para un descubrimiento de nivel 1, el nombre de dominio completo es el resultado de una búsqueda inversa de la dirección IP. Esta búsqueda utiliza una biblioteca resolver que proporciona el sistema operativo y utiliza cualquier configuración que aquí se proporcione. Por ejemplo, si, en el nivel del sistema operativo, se prefiere el archivo host en lugar del sistema de nombres de dominio (DNS), primero se considerará la información del archivo hosts.

Para un descubrimiento de nivel 2, TADDM realiza una búsqueda inversa de todas las dirección IP descubiertas mediante la biblioteca resolver que proporciona el sistema operativo. De nuevo, la configuración del sistema operativo dicta de dónde obtiene la información la búsqueda inversa. Si el sistema de nombres de dominio (DNS) no está configurado o el sistema de nombres de dominio (DNS) devuelve nombres de dominio totalmente calificados, puede utilizar el archivo hosts para sustituirlo.

Una que se han buscado las direcciones IP descubiertas, se realiza un intento de coincidencia entre el nombre de dominio completo y el sistema informático. Existen diferentes maneras de obtener un nombre de dominio completo y se intenta cada uno de los métodos, en un orden predefinido, hasta que se encuentra un nombre de dominio completo válido. Puede modificar el orden para que el método preferido tenga mayor prioridad. Están disponibles los siguientes métodos:

Método 1

TADDM selecciona el nombre de dominio completo de una interfaz de IP en la que la parte de host del nombre de dominio completo coincide con el nombre de host del sistema descubierto. Si hay varias coincidencias, el nombre de dominio completo seleccionado depende de la prioridad del nombre de dominio definido en la propiedad: `com.collation.platform.os.FqdnPriorities`. Esta prioridad incluye los nombres de dominio en orden de prioridad. Para priorizar los dominios, especifique el nombre de los dominios como una lista separada por comas en una sola línea:

```
com.collation.platform.os.FqdnPriorities=domain1.company.com,
domain2.company.com,domain3.company.com
```

El nombre de dominio completo con la prioridad más alta de su dominio se devuelve como el nombre de dominio completo. Este método utiliza la información descubierta acerca de los nombres de dominios totalmente calificados de las interfaces y de los nombres de sistemas informáticos.

Si no se definen las prioridades, TADDM pasa por todas las interfaces IP. TADDM comprueba si el nombre de dominio completo asociado con una interfaz IP equivale al nombre del sistema informático o si el fragmento del nombre de host de este nombre de dominio completo equivale al nombre del sistema informático. El primer nombre de dominio completo que coincida con los criterios se devuelve como el nombre de dominio completo.

Por ejemplo, supongamos que un sistema informático llamado “myname” tiene dos interfaces con los siguientes nombres de dominio completos:

- interface #1 myname.domain1.com
- interface #2 myname.domain2.com

Si no se ha definido `com.collation.platform.os.FqdnPriorities`, la primera coincidencia se devuelve como el nombre de dominio completo. En ambos nombres, el fragmento de host del nombre de dominio completo coincide con el nombre de host del sistema descubierto, pero el nombre de dominio completo devuelto es “myname.domain1.com”. Para priorizar el nombre que debe seleccionarse, utilice la propiedad `com.collation.platform.os.FqdnPriorities`. Por ejemplo si la entrada `com.collation.platform.os.FqdnPriorities` contiene la siguiente información:

```
com.collation.platform.os.FqdnPriorities=domain2.com,domain1.com
```

En este caso, el nombre de dominio completo devuelto es “myname.domain2.com”, porque este nombre tiene una prioridad más alta.

Método 2

Propiedad `com.collation.platform.os.command.fqdn` especifica un mandato externo en el servidor de TADDM que se utiliza para hacer las búsquedas inversas. En los ejemplos siguientes se muestra cómo utilizar esta propiedad; especifique la propiedad en una sola línea:

```
com.collation.platform.os.command.fqdn=nslookup $1
| grep Name | awk '{print $2}'
com.collation.platform.os.command.fqdn.AIX=nslookup $1
| grep Name | awk '{print $2}'
com.collation.platform.os.command.fqdn.Linux=nslookup $1
| grep Name | awk '{print $2}'
com.collation.platform.os.command.fqdn.SunOS=nslookup $1
| grep Name | awk '{print $2}'
com.collation.platform.os.command.fqdn.Windows=nslookup $1
```

Método 3

Propiedad `com.collation.platform.os.command.hostOfHostname` especifica un mandato externo en el sistema de destino que se utiliza para proporcionar el nombre de dominio completo. En el ejemplo siguiente, se muestra cómo utilizar esta propiedad en un sistema UNIX; especifique la propiedad en una sola línea:

```
com.collation.platform.os.command.hostOfHostname=host `hostname`
| awk {'print $1'}
```

Método 4

Se utiliza el nombre de dominio completo de la interfaz primaria. La interfaz IP primaria se especifica como el valor IP más bajo, donde los valores IP están ordenados de forma descendente.

Método 5

Se utiliza la dirección IP de la interfaz primaria.

Método 6

Se utiliza el nombre del sistema informático.

Método 7

Establezca la IP de contexto de sesión.

Método 8

Establezca FQDN para CS como FQDN para la IP de sesión.

Puede definir el orden en el se intentan estos métodos definiendo la propiedad `com.collation.platform.os.fqdnSearchOrder`. El valor de esta propiedad es una lista separada por comas de los números de estos métodos. El valor predeterminado es 1,2,3,4,5,6,7,8. En este caso, TADDM intenta primero utilizar el método 1. Si éste no devuelve un nombre de dominio completo válido, intenta el método 2 y así sucesivamente, hasta que obtenga un nombre de dominio completo válido y se detenga. Un nombre de dominio completo válido es un nombre que se ajusta a las normas especificadas en el RFC 1035.

Esta solución también es aplicable para los sistemas informáticos que se descubren a través del uso de sensores de protocolo simple de gestión de red. Puede definir qué soluciones tendrán mayor prioridad y, por lo tanto, que se pueden utilizar para encontrar un nombre de dominio completo más rápidamente.

En todos los casos, el sistema de nombres de dominio configurado correctamente es el método preferido para definir nombre de host. Si el sistema de nombres de dominio no se puede utilizar, utilice el archivo hosts. El uso del sistema de nombres de dominio (DNS) o de archivos hosts son las maneras estándar de proporcionar resolución de nombres para las direcciones IP. TADDM proporciona formas de sustituir estos métodos, pero como ningún otro método es exclusivo para TADDM, tendrán que conducir a nombres que sean coherentes con nombres de sistemas de gestión.

Seguimiento de un descubrimiento

Puede realizar un seguimiento de las fases del descubrimiento desde el inicio del descubrimiento hasta el momento en que se actualiza el historial de cambios y se compilan las dependencias de topología. Cada fase de un descubrimiento se registra en un archivo de registro asociado.

Fase de ejecución del descubrimiento y archivo de registro

Una vez iniciado un descubrimiento, a cada descubrimiento se le asigna un identificador exclusivo (ID de ejecución). Una indicación de la hora *AAAA-MM-DD-hh:mm:ss:SSS* identifica la ejecución del descubrimiento, por ejemplo, `20110517225225948`. La parte *AAAA-MM-DD* representa el año, mes y día. La parte *hh:mm:ss.sss* representa la hora del día en formato de reloj de 24 horas, contado en milésimas de segundo. En el ejemplo anterior, la fecha es 2011/05/17 y la hora es 22:52:25.948. Puede utilizar este identificador para crear archivos de registro separados para cada sensor del directorio `$COLLATION_HOME/log/sensors`. La indicación de la hora se utiliza en los archivos de registro.

Durante un descubrimiento, el gestor de flujos de procesos supervisa el estado del descubrimiento y el estado de los sucesos del sensor. El gestor del flujo de procesos también gestiona el traspaso de un servicio a otro. La actividad del flujo del proceso se almacena en el archivo `$COLLATION_HOME/log/services/ProcessFlowManager.log` del servidor de dominio o descubrimiento.

Los siguientes ejemplos muestran diferentes actividades supervisadas por el gestor de flujos de procesos y cómo se almacena esta información en el archivo de registro.

Inicio del descubrimiento:

```
– 2011-05-17 22:53:01,643 ProcessFlowManager [RMI TCP Connection(42)-127.0.0.1] INFO
processflowmgr.ProcessFlowManagerImpl - [ProcessFlowManagerImpl.I.0] startDiscovery()
started discovery with run id 2,011,051,722,525,948
– 2011-05-17 22:53:01,643 ProcessFlowManager [RMI TCP Connection(42)-127.0.0.1] INFO
processflowmgr.ProcessFlowManagerImpl - [ProcessFlowManagerImpl.I.22] startDiscovery()
 setting the discoveryRun's run id to 2,011,051,722,525,948
– 2011-05-17 22:53:01,973 ProcessFlowManager [RMI TCP Connection(42)-127.0.0.1] INFO
processflowmgr.ProcessFlowManagerImpl -
Discovery run, 2011051722525948 started with profile Level 2 Discovery
```

Descubrimiento realizado:

```
– 2011-05-17 22:56:11,689 ProcessFlowManager [RMI TCP Connection(45)-127.0.0.1] INFO
processflowmgr.ProcessFlowManagerImpl - [ProcessFlowManagerImpl.I.36]
discoveryDone(2,011,051,722,525,948) called by Discovery Manager
```

Suceso de descubrimiento:

```
- 2011-05-17 22:53:49,901 ProcessFlowManager [RMI TCP Connection(45)-127.0.0.1] INFO
processflowmgr.ProcessFlowManagerImpl - [ProcessFlowManagerImpl.I.32]
discoveryProgress(2,011,051,722,525,948, Discovered - The CustomAppServerSensor
(JavaServer 9.156.47.175:36750) sensor discovered the following: CustomAppServerResult,
 JavaServer,9.156.47.175:36750.) called by Discovery Manager
```

Fase del compilador de topología y del archivo de registro

El compilador de topología compila las relaciones y dependencias entre los elementos descubiertos. El compilador de topología ejecuta una lista de agentes que se listan en el archivo `$COLLATION_HOME/etc/TopologyBuilderConfigurationDefault.xml`. Los agentes de topología se ejecutan en intervalos especificados. No obstante, los sucesos que se producen durante un descubrimiento y cuando se completa un descubrimiento también pueden desencadenar el compilador de topología. Cada agente lleva a cabo una tarea específica, por ejemplo, consolida, calcula las dependencias, compila los diagramas de dependencias y elimina la información antigua. Los archivos de registro del

compilador de topologías se almacenan en los archivos $COLLATION_HOME/log/services/TopologyBuilder.log y $COLLATION_HOME/log/agents/*.log del servidor de dominio, el servidor de sincronización y el servidor de almacenamiento primario.

Los ejemplos siguientes muestran las diferentes etapas de compilación de relaciones y cómo se almacena esta información en el archivo de registro.

Inicio de la ejecución del compilador:

```
– 2011-05-17 22:56:11,717 TopologyBuilder [RMI TCP Connection(158)-127.0.0.1]
INFO cdb.TivoliStdMsgLogger
- CTJOT0400I Topology builder is starting.
```

Compilador de topología finalizado:

```
– 2011-05-17 23:16:39,429 TopologyBuilder
[TopologyBuilderEngineThread$Dependency@0.5]
 INFO engine.TopologyBuilderEngine - Topology agent completed :
 all normally in seconds 30.367
```

Paso al siguiente agente de topología:

```
– 2011-05-17 23:16:29,774 TopologyBuilder [TopologyBuilderEngineThread$Dependency@0.5]
INFO cdb.TivoliStdMsgLogger - CTJOT0403I Topology builder agent class
com.ibm.cdb.topomgr.topobuilder.agents.ComputerSystemConsolidationAgent is stopping.
– 2011-05-17 23:16:30,078 TopologyBuilder [TopologyBuilderEngineThread$Dependency@0.5]
INFO cdb.TivoliStdMsgLogger - CTJOT0402I Topology builder agent class
com.ibm.cdb.topomgr.topobuilder.agents.ComputerSystemTypeAgent is starting.
```

Si encuentra algún problema, por ejemplo, si se cuelga el compilador de topología, busque en el archivo de registro el último agente de topología iniciado para identificar el problema. Si no hay entradas en el archivo TopologyBuilder.log, compruebe las entradas en el archivo TopologyManager.log después de la indicación de la hora del último agente iniciado. Si sabe qué agentes causan los problemas, puede revisar también el archivo $COLLATION_HOME/log/agents/agentName.log para identificarlos.

Otros servicios y archivos de registro

El gestor de cambios procesa los sucesos y actualiza los registros del historial de cambios. Este proceso es independiente de la fase de descubrimiento. Recibe los sucesos de otros servicios, por ejemplo, el proceso del compilador de topología y el programa de carga masiva. Cuando abre una vista de topología, el gestor de vistas compila las estructuras necesarias para la GUI de modo que muestren la topología de forma eficaz. Los registros de servicios se almacenan en el directorio $COLLATION_HOME/log/services. Cada registro de servicio tiene el mismo nombre que el servicio, por ejemplo, el archivo services/ChangeManager.log.

Los siguientes ejemplos muestran cómo se almacena esta información en los archivos del registro de servicios.

ChangeManager:

```
2011-05-19 13:22:42,342 ChangeManager [ChgWork-1] INFO changemgr.
ChangeManagerPersisterImpl -
[ChangeManagerPersister.I.3] Got a create or delete event
```

ViewManager:

```
2011-05-19 16:37:22,428 ViewManager [RMI TCP Connection(174)-127.0.0.1]
INFO viewmgr.ViewMetaLoader - [ViewMetaLoader.I.31] getViewMeta()
found view meta definition for view Business Application Topology
```

Almacenamiento en memoria caché de las últimas credenciales correctas

TADDM puede almacenar en memoria caché las últimas credenciales de acceso que han funcionado. Se pueden volver a utilizar durante el siguiente descubrimiento (Nivel 2 o basado en script).

Durante el descubrimiento inicial de un destino, el servidor TADDM itera por la lista de acceso y valida cada elemento en relación con el destino de la operación de descubrimiento. Cuando se encuentran credenciales válidas, se clasifican en una memoria caché y se vuelven a utilizar durante los descubrimientos consecutivos del mismo destino de descubrimiento.

Una memoria caché puede almacenar los dos valores siguientes:

credenciales
: Este valor se almacena en una memoria caché cuando se encuentran las credenciales válidas para un destino de descubrimiento durante la operación de descubrimiento. Durante el siguiente descubrimiento, éstas se leen en la memoria caché y se comprueba si continúan siendo válidas. Si continúan siendo válidas, se utilizan para el descubrimiento. Si ya no son válidas y se ha inhabilitado la reserva, la información acerca de que ha fallado el último intento se almacena en el servidor y se detiene el descubrimiento. Cuando está habilitada la reserva, el servidor itera por la lista de acceso e intenta encontrar nuevas credenciales válidas. Para habilitar la reserva, establezca la propiedad `com.ibm.cdb.security.auth.cache.fallback.failed` en `true`.

la información acerca del último intento fallido (junto con el último error)
: Este valor se almacena en una memoria caché cuando no se encuentran las credenciales válidas para un destino de descubrimiento durante la operación de descubrimiento. Si se ha inhabilitado la reserva, se visualiza la información acerca de que ha fallado el último intento y se detiene el descubrimiento. Si está habilitada la reserva, el servidor itera por la lista de acceso e intenta encontrar nuevas credenciales válidas. Para habilitar la reserva, establezca la propiedad `com.ibm.cdb.security.auth.cache.fallback.invalid` en `true`.

De forma predeterminada, la reserva está habilitada en ambos casos. Puede personalizar el comportamiento de la reserva y el almacenamiento en memoria caché de las credenciales estableciendo adecuadamente las propiedades de almacenamiento en memoria caché de las credenciales de acceso.

Nota: Las credenciales se almacenan en memoria caché por dirección IP, etiqueta de ubicación, tipo de credencial y protocolo utilizado durante la conexión. Cuando se elimina la entrada de acceso, también se eliminan las entradas almacenadas en memoria caché asociadas. La memoria caché de credenciales se puede gestionar mediante el nuevo programa de utilidad cachemgr.

Limitaciones

- El almacenamiento en memoria caché de las credenciales no se utiliza en el descubrimiento de nivel 3. Solo se utiliza para el descubrimiento de sistema de nivel 2 y para los sensores basados en scripts.
- Una memoria caché no realiza un seguimiento de los cambios de restricciones de acceso al ámbito. Por ejemplo, si un destino de descubrimiento está dentro de la restricción de acceso al ámbito, se descubre y se almacena en memoria caché y, a continuación, se traslada fuera de la restricción del ámbito, el valor almacenado en memoria caché se continúa utilizando.
- El valor almacenado en memoria caché tiene prioridad sobre la lista de acceso de perfiles. Por ejemplo, si ejecuta el descubrimiento utilizando la lista de acceso principal y se almacenan credenciales válidas, el valor de la memoria caché se continúa utilizando incluso si especifica otras credenciales en un perfil.

Puede eliminar un valor almacenado en memoria caché mediante el programa de utilidad cachemgr. Si con frecuencia utiliza perfiles diferentes con entradas de acceso diferentes para el mismo destino o ámbito de descubrimiento, puede inhabilitar el almacenamiento en memoria caché para los mismos. De lo contrario, es posible que se utilicen credenciales erróneas en el descubrimiento.

Visión general del proceso de compilación de topologías

TADDM ejecuta el proceso de construcción de topología de forma periódica. Hasta que se completa el proceso de compilación de topologías después del descubrimiento o después del funcionamiento de carga en bloque, pueden existir objetos sin reconciliar en la base de datos de TADDM y las relaciones de las topologías pueden estar incompletas.

Este proceso es el mismo independientemente del tipo de despliegue de TADDM que se utilice.

La compilación de topología incluye las siguientes operaciones:

Limpieza de la base de datos de TADDM
Proceso que suprime las entidades antiguas, elimina las dependencias que son orígenes o destinos con carencias y elimina otros elementos que están reemplazados.

Establecimiento de dependencias entre los elementos de configuración
Proceso que crea dependencias entre los procesos en comunicación, por ejemplo entre una aplicación y la base de datos subyacente y entre las colas de WebSphere MQ remitentes y receptoras. Además se establecen dependencias entre componentes de un clúster de una aplicación o simplemente entre dos sistemas informáticos.

Creación y aumento de elementos de configuración
Proceso que utiliza información procedente de elementos de configuración y conexiones para sintetizar los nuevos elementos de configuración. Por ejemplo, es posible que TADDM cree un elemento de configuración nuevo denominado “ApplicationServerClusters” y que esté basado en la información derivada de descubrimientos anteriores y operaciones de carga en bloque.

Creación de información para vistas de topología
Proceso que genera y almacena información que el Portal de gestión de datos puede utilizar para mostrar más rápidamente las vistas de topologías.

Exportación de datos
El proceso pide a la base de datos de TADDM que exporte la información de los elementos de configuración a sistemas externos. Por ejemplo, la integración con los servicios de registro se implementa como un agente de topología.

Archivos de registro y registro

La *Guía de resolución de problemas* de TADDM y los temas que incluye describen los archivos de registro de TADDM y cómo configurar el registro para resolver problemas.

Protección del entorno

En entornos seguros, TADDM fuerza la autenticación para ayudar a proteger la información confidencial.

Puede utilizar el portal de gestión de datos para configurar las cuentas de usuario. Cada usuario debe tener una cuenta de usuario válida para utilizar el portal de gestión de datos para acceder a la información descubierta sobre los componentes de infraestructura y red.

Cuando inicie sesión en la consola de Discovery Management y seleccione la opción **Establecer una sesión segura (SSL)** se cifran todos los datos (incluidos los nombres de usuario y las contraseñas) antes de enviar los datos por la red.

En el proceso de descubrimiento, el servidor de TADDM utiliza el protocolo Secure Shell (SSH) para comunicarse con seguridad con todos los hosts y otros dispositivos que dan soporte a SSH.

El servidor soporta la autenticación de SSH basada en clave y la autenticación de SSH basada en contraseña y en registro. Cuando se utiliza la autenticación de SSH basada en contraseña y en registro, se utilizan los nombres de usuario y contraseñas definidos en la lista de acceso para iniciar sesión en los hosts de los sistemas que se van a descubrir.

Consulte también “Propiedades de seguridad” en la página 96.

Control del acceso de usuario a los elementos de configuración

TADDM controla el acceso de los usuarios a elementos de configuración mediante el uso de colecciones de acceso, roles y permisos.

El control de accesos de elementos de configuración se establece mediante el proceso siguiente:

1. Se añaden elementos de configuración a las colecciones de accesos.
2. Se definen roles que añaden conjuntos de permisos.
3. Se definen usuarios o grupos de usuarios y se asignan roles a cada usuario o grupo de usuarios para otorgar permisos específicos (para colecciones de accesos específicas) a dicho usuario.

En el contexto de la seguridad de TADDM, un usuario es una persona a la que se le ha otorgado acceso a los elementos de configuración y un grupo de usuarios son varios usuarios que tienen los mismos roles y permisos.

Puede crear usuarios y grupos de usuarios en el Portal de gestión de datos. El acceso de los usuarios de los grupos de usuarios a elementos de configuración se define mediante los roles y las colecciones de accesos que se asignan a dicho usuario o grupo de usuarios. Puede cambiar estas asignaciones en cualquier momento.

Permisos

Un permiso autoriza al usuario a realizar una acción o a acceder a un elemento de configuración específico. Los permisos se agregan a los roles y estos permisos se otorgan a los usuarios asignándoles roles que tengan esos permisos.

TADDM proporciona cuatro permisos, cada uno de los cuales se clasifica como un permiso de nivel de datos o un permiso de nivel de método.

Permisos de nivel de datos

Los permisos de lectura y actualización son permisos de nivel de datos.

Lectura
El usuario puede visualizar información sobre un elemento de configuración.

Actualización
El usuario puede modificar la información sobre un elemento de configuración.

Permisos de nivel de método

Los permisos de descubrimiento y administración son permisos de nivel de datos.

Descubrir
El usuario puede iniciar un descubrimiento, crear y actualizar objetos de ámbito de descubrimiento o crear nuevos objetos, por ejemplo, desde el menú Editar de la consola de Discovery Management.

Un usuario sin el permiso de descubrimiento no puede iniciar sesión en la consola de Discovery Management ni ver el separador Descubrimiento en Data Management Portal.

Administrador
El usuario puede crear o actualizar usuarios, roles y permisos. El usuario también puede configurar la política de autorización con el gestor de autorización.

Habilitación de la seguridad de nivel de datos

Puede habilitar la seguridad de nivel de datos para los sistemas operativos AIX, Linux, Linux en System z y Windows mediante el archivo `collation.properties`.

Para habilitar la seguridad de nivel de datos de manera que pueda otorgar permisos de lectura y actualización de forma selectiva, siga estos pasos:

1. En el archivo `collation.properties`, localice la línea siguiente y cambie el valor de la propiedad de `false` a `true`:
   ```
   com.collation.security.enabledatalevelsecurity=false
   ```
2. Guarde el archivo.
3. Detenga el servidor de TADDM.
4. Reinicie el servidor de TADDM.

Nota: En un despliegue de servidor en modalidad continua, debe actualizar el archivo `collation.properties` en cada servidor de almacenamiento y reiniciar reinicia cada uno de ellos.

Puede definir más permisos granulares creando colecciones de accesos. Si la seguridad a nivel de datos está habilitada, se pueden asegurar los recursos de TADDM principales utilizando colecciones de accesos. Si está habilitada la seguridad en el nivel de datos, los usuarios pueden modificar solo los elementos de configuración contenidos en colecciones de accesos para las que tengan permiso de actualización.

Los recursos auxiliares, como los recursos geográficos y físicos, incluido el atributo `SiteInfo`, no se visualizan al crear la colección de accesos.

Roles

Un rol es un conjunto de permisos que se pueden asignar a un usuario. Asignar un rol otorga la posibilidad de acceso específico.

Cuando asigne un rol a un usuario, debe especificar una o más colecciones de accesos para dicho rol. Esto limita el ámbito del rol a sólo una de estas colecciones de accesos que es la apropiada para ese usuario.

Por ejemplo, Sarah es la responsable de las estaciones de trabajo y los servidores y estaciones de trabajo NT de su empresa, así que le asigna el rol de supervisor en una colección de accesos que contiene estos sistemas. Jim es el responsable de los sistemas Linux; y usted le asigna el rol de supervisor en una colección de accesos que contenga esos sistemas. Aunque se les ha asignado el mismo rol a Sarah y Jim (debido a que realizan las mismas operaciones), tienen acceso a diferentes recursos.

Nota: Si está utilizando un servidor de sincronización, deberá crear el rol para cada dominio TADDM y sincronizar los servidores del dominio con el servidor de sincronización.

Roles predefinidos

TADDM proporciona los siguientes roles predefinidos:

operador
: Este rol tiene permiso de lectura.

supervisor
: Este rol tiene permisos de lectura, actualización y descubrimiento.

administrador
: Este rol permisos de lectura, actualización, descubrimiento y administración.

Roles adicionales que puede crear

Puede crear roles adicionales para asignar otras combinaciones de permisos. Las siguientes combinaciones pueden resultar especialmente útiles:

Lectura + Actualización
: Permiso para leer y actualizar objetos de las colecciones de acceso asignadas.

Lectura + Actualización + Administración
: Permiso para leer y actualizar objetos de las colecciones de accesos asignadas, y para crear usuarios, roles y permisos.

Colecciones de accesos

TADDM no gestiona el acceso a los elementos de configuración de forma individual. En su lugar, los elementos de configuración se agregan en conjuntos denominados colecciones de accesos. Una colección de accesos es un conjunto de elementos de configuración que se gestiona de forma colectiva con fines de seguridad.

La seguridad de cada colección de accesos se gestiona mediante la creación de roles y la asignación de éstos a los usuarios. El rol se aplica sólo a las colecciones

de accesos que se especifiquen al asignar el rol a un usuario. Las colecciones de accesos se utilizan para limitar el ámbito del rol.

Cuando instala TADDM, se crea la colección de accesos denominada `DefaultAccessCollection`, que contiene todos los elementos de configuración. Todos los usuarios tienen permiso de lectura y de actualización para esta colección de accesos de manera predeterminada, a menos que se haya activado la seguridad de nivel de datos.

Nota: Los usuarios no tienen permisos para leer y actualizar las colecciones de accesos; sólo pueden leer y actualizar elementos de configuración individuales. Sin embargo, los usuarios tienen permisos de lectura y actualización para aquellas colecciones de accesos que son miembros de colecciones de acceso asignadas.

Restablecimiento de las políticas de seguridad

Si es necesario restablecer las políticas de seguridad (permisos, roles y colecciones de accesos) a su estado predeterminado, podrá hacerlo sustituyendo dos archivos. Sin embargo, el restablecimiento de políticas de seguridad requiere que suprima y vuelva a crear todos los usuarios.

Acerca de esta tarea

Las políticas de seguridad se almacenan en los siguientes dos archivos del directorio `$COLLATION_HOME/var/policy` y estos archivos se utilizan para inicializar las políticas de seguridad:

- `AuthorizationPolicy.xml`
- `AuthorizationRoles.xml`

Una vez que se han inicializado las políticas de seguridad, estos archivos se renombran y se almacenan en el mismo directorio. Por ejemplo, se ha cambiado el nombre de los archivos siguientes:

- `AuthorizationPolicy.backup.xml`
- `AuthorizationRoles.backup.xml`

Las versiones predeterminadas de los archivos, que contienen las políticas de seguridad suministradas, se encuentran en el mismo directorio. Los archivos siguientes son las versiones predeterminadas:

- `DefaultPolicy.xml`
- `DefaultRoles.xml`

Procedimiento

Para restaurar las políticas de seguridad predeterminadas, efectúe los pasos siguientes:

1. Para guardar los archivos de políticas actuales, cambie el nombre o muévalos a un directorio diferente.
2. Suprima los usuarios que haya creado.
3. Suprima el directorio `$COLLATION_HOME/var/ibmsecauthz`.
4. Cree una copia del archivo `DefaultPolicy.xml` y asígnele el nombre `AuthorizationPolicy.xml`.
5. Cree una copia del archivo `DefaultRoles.xml` y asígnele el nombre `AuthorizationRoles.xml`.
6. Reinicie el servidor.

7. Según convenga, cree usuarios.

Bloqueos

Puede utilizar bloqueos para bloquear el uso a un usuario individual o a todos los usuarios para que no usen TADDM si se supera el número configurado de intentos de inicio de sesión. El uso de la función de bloqueo proporciona un mejor control de la autenticación y ayuda a evitar el pirateo de contraseña.

Un bloqueo local se desencadena si un usuario individual supera el número configurado de intentos de inicio de sesión fallidos. Como resultado, el usuario no puede iniciar la sesión en TADDM durante un periodo de tiempo configurado.

Si se desencadena un bloqueo global, ningún usuario puede iniciar la sesión en TADDM durante un periodo de tiempo configurado. Un bloqueo global lo desencadena una de las dos situaciones siguientes:

- El número de bloqueos activos para distintos usuarios de supera el número configurado de bloqueos globales máximos permitidos.
- El número de intentos de inicio de sesión fallidos para nombres de usuario únicos supera el límite configurado.

Cuando se desencadena un bloqueo, las sesiones existentes no resultan afectadas.

Puede especificar el número de intentos de inicio de sesión fallidos permitidos y el periodo de tiempo durante el que un bloqueo permanece activo mediante la configuración de propiedades en el archivo `collation.properties`. Para obtener más información sobre estas propiedades, consulte “Propiedades de bloqueo” en la página 93.

Cuando transcurre el tiempo de un bloqueo global, todos los bloqueos local en curso se borran de manera automática.

En un despliegue de servidor de sincronización, el servidor de sincronización controla la seguridad de todos los dominios de TADDM. Todos los bloqueos que estuvieran activos en el servidor de dominio antes de que se conectara al servidor de sincronización se borran cuando la sincronización entre el servidor de dominio y el servidor de sincronización se habilita.

Los intentos de inicio de sesión fallidos que cuentan para el total pueden ser de cualquier tipo, por ejemplo, mediante la API de CLI, la API de Java, herramientas (scripts), SOAP, REST, Discovery Management Console o el Portal de gestión de datos. La función de bloqueo se aplica a integraciones que utilizan la API de TADDM, pero no se aplica a inicios de sesión que utilicen inicio de sesión único o integraciones basadas en base de datos, como, por ejemplo, Tivoli Common Reporting.

Un administrador de servidor de TADDM puede borrar un bloqueo local o global mediante el script `$COLLATION_HOME/bin/lockmgr.sh`. Puede ejecutar el script desde los siguientes servidores:

- Servidor de dominio, en un despliegue de servidor de dominio
- Servidor de sincronización, en un despliegue de servidor de sincronización
- Servidor de almacenamiento primario, en un despliegue de servidor en modalidad continua

Puede ejecutar el script `lockmgr.sh` con los siguientes servidores:

lockmgr.sh -s
Visualiza el estado del bloqueo.

lockmgr.sh -g
Borra un bloqueo global activo.

lockmgr.sh -u *nombre_usuario*
Borra un bloqueo local activo para un usuario concreto.

lockmgr.sh -h
Muestra información de ayuda para el script `lockmgr.sh`.

Cifrado

El cifrado es el proceso de transformación de datos en un formato ininteligible de tal modo que, o bien no se puedan obtener los datos originales, o bien sólo se puedan obtener mediante un proceso de descifrado.

Fix Pack 5 TADDM utiliza la propiedad '*com.collation.security.algo.aes.keylength*' para decidir el algoritmo (AES 128 o AES 256) del proveedor de seguridad '*FIPS-compliant IBMJCEFIPS*' para cifrar los siguientes elementos:

- Las contraseñas, incluidas las entradas de los archivos `collation.properties` y `userdata.xml`.
- Las entradas de lista de acceso almacenadas en la base de datos.

Por ejemplo:

Esta propiedad define la longitud de clave para AES `-com.collation.security.algo.aes.keylength=128`.

Cuando se instala TADDM por primera vez, se genera una clave de cifrado, y las contraseñas se cifran mediante esta nueva clave de cifrado. La ubicación predeterminada de la clave de cifrado es el archivo `etc/TADDMSec.properties`.

Cambio de la ubicación de la clave de cifrado de TADDM

Para cambiar la ubicación del archivo de claves, cambie el valor de la propiedad `com.collation.security.key` en el archivo `collation.properties`. Puede definir la propiedad en otra ubicación relativa al directorio `$COLLATION_HOME`.

Para evitar la pérdida de datos, guarde una copia de seguridad de la clave de cifrado en una ubicación diferente. Esta puede restaurarse si se produce un problema en la copia original.

Cambio de la clave de cifrado de TADDM en un despliegue de servidor de dominio

Nota: TADDM no soporta el cambio de la clave de cifrado después de la instalación en un despliegue de servidor en modalidad continua y un despliegue de servidor de sincronización.

Para cambiar la clave de cifrado de TADDM en un despliegue de servidor de dominio, utilice el script `bin/changekey.sh` (o un archivo de script por lotes equivalente). Este script migra las entradas cifradas de los archivos `collation.properties` y `userdata.xml`, y también las entradas de la lista de acceso almacenadas en la base de datos. Para utilizar el script `bin/changekey.sh`, asegúrese de que ha iniciado sesión como el usuario no root definido durante la instalación.

Si el script tiene éxito, es necesario reiniciar TADDM.

Formato para la ejecución del script

```
./changekey.sh $COLLATION_HOME usuario_administrador contraseña
```

Ejemplo

```
./changekey.sh /opt/IBM/taddm/dist administrator taddm
```

Compatibilidad con FIPS

Puede configurar TADDM para que pueda funcionar en una modalidad que utilice algoritmos compatibles con FIPS para el cifrado, estableciendo la propiedad FIPSMode **com.collation.security.FIPSMode** en `true`.

Establecer la propiedad **com.collation.security.FIPSMode** en `true` en los archivos siguientes:

- `$COLLATION_HOME/dist/etc/collation.properties`
- `$COLLATION_HOME/dist/sdk/etc/collation.properties`
- `sdk/etc/collation.properties` de cada una de las instalaciones de SKD de TADDM que se conectan al TADDM compatible con FIPS.

El valor predeterminado de la propiedad **com.collation.security.FIPSMode** es `false`.

Cuando se encuentra en la modalidad FIPS, TADDM utiliza los siguientes proveedores criptográficos aprobados para FIPS 140-2:

- IBMJCEFIPS (certificado 376)
- IBMJSSEFIPS (certificado 409)

Para obtener más información sobre los certificados 376 y 409, consulte el sitio web del National Institute of Standards and Technology (NIST), http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2004.htm.

La modalidad FIPS puede utilizarse con todos los tipos de descubrimientos de TADDM, con las siguientes excepciones:

- Descubrimiento de SNMP de nivel 2
- Descubrimiento de i5/OS de nivel 2
- Descubrimiento de ZEnterprise nivel 2
- Descubrimiento de VMware ESXi de nivel 2
- Descubrimiento de VMware Virtual Center de nivel 3
- Descubrimiento de JBoss de nivel 3
- Descubrimiento de Oracle Application Server de nivel 3
- Descubrimiento de WebLogic de nivel 3
- Descubrimiento de SAP CCMS y SLD de nivel 3
- Descubrimiento de EMC de nivel 3
- Fix Pack 1 Descubrimiento de Sybase de nivel 3
- Los descubrimientos de nivel 2 y 3 donde se utiliza Windows Management Instrumentation (WMI) o la sesión de PowerShell (la sesión de PowerShell está soportada en TADDM 7.3.0.2 o posterior) para descubrir plataformas Windows, solo si el servidor de TADDM de Windows, las pasarelas de Windows y los destinos de descubrimiento de Windows no se ejecutan en modalidad compatible con FIPS. Para configurar los servidores de Windows para que se ejecuten en la modalidad compatible con FIPS, consulte la documentación de Windows, por ejemplo, http://support.microsoft.com/kb/811833.

Cuando está en la modalidad FIPS, los sensores de TADDM que utilizan SSH no se pueden conectar a los servidores que sólo dan soporte al protocolo SSHv1 o al protocolo SSHv2 con cifrados demasiado débiles. TADDM no puede verificar si la implementación de SSH en los servidores de destino es compatible con FIPS. Debe comprobar si las implementaciones de SSH que utiliza en su entorno son compatibles con FIPS.

En la modalidad FIPS, cuando utiliza SDK de TADDM y la consola de Discovery Management en la modalidad segura, sólo está soportado IBM Java.

Conceptos relacionados:

"Conformidad con SP800-131"
Puede configurar TADDM para que dé soporte al estándar de seguridad del Instituto Nacional de Estándares y Tecnología (NIST) SP800-131a.

Conformidad con SP800-131

Puede configurar TADDM para que dé soporte al estándar de seguridad del Instituto Nacional de Estándares y Tecnología (NIST) SP800-131a.

El estándar de seguridad SP800-131a requiere longitudes de clave más largas y una criptografía más potente que otros estándares, por ejemplo, el estándar FIPS 140-2. Se requiere también la seguridad de la capa de transporte (TLS) v1.2. Para obtener más información, consulte http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf.

⌂ Para habilitar la modalidad P800-131a establezca la propiedad `com.ibm.jsse2.sp800-131` en `strict` en los archivos siguientes:

- `$COLLATION_HOME/dist/etc/collation.properties`
- `$COLLATION_HOME/dist/sdk/etc/collation.properties`
- `sdk/etc/collation.properties` de cada instalación del SDK de TADDM que se conecta al TADDM compatible con SP800-131.

De forma predeterminada, la propiedad `com.ibm.jsse2.sp800-131` no está establecida.

La modalidad de conformidad SP800-131a está soportada para los mismos tipos de descubrimientos de TADDM que la modalidad FIPS.

En la modalidad SP800-131, TADDM utiliza el protocolo SSL más seguro (TLS v1.2) en la comunicación cifrada. Asegúrese de que se cumplan los siguientes requisitos.

- Cuando utiliza Data Management Portal a través del puerto SSL web (HTTPS), primero debe configurar el navegador web para que dé soporte al protocolo TLS v1.2.
- Cuando utiliza SDK de TADDM y la consola de Discovery Management en la modalidad segura, debe habilitar el protocolo TLS v1.2 en Java Runtime Environment. Asimismo, sólo IBM Java está soportado.
- Cuando el certificado SSL no cumple el estándar SP800-131a, debe volver a crearlo. Para ver los pasos necesarios, consulte "Instalación de certificados SSL personalizados para utilizarlos en TADDM" en la página 35.

Conceptos relacionados:

"Compatibilidad con FIPS" en la página 23
Puede configurar TADDM para que pueda funcionar en una modalidad que utilice algoritmos compatibles con FIPS para el cifrado, estableciendo la propiedad FIPSMode **`com.collation.security.FIPSMode`** en `true`.

Seguridad para un despliegue de servidor de sincronización

Si utiliza un despliegue de servidor de sincronización, debe realizar cambios de seguridad cuando configure el servidor de sincronización para su entorno.

Si utiliza un registro basado en archivo de TADDM y se añade un dominio de TADDM al servidor de sincronización, debe volver a crear en el servidor de sincronización cualquier usuario que ya exista en el dominio, incluidos los roles y accesos otorgados a las colecciones de accesos. Si utiliza un protocolo Lightweight Directory Access Protocol (LDAP) o un registro de usuario de repositorios federados WebSphere, debe añadir al servidor de sincronización cualquier usuario que acceda a TADDM.

Cuando se añade un dominio al servidor de sincronización, la autenticación y autorización para el nuevo dominio se delega al servidor de sincronización.

Los inicios de sesión al dominio se procesan en el servidor de sincronización. Ademas, las llamadas de método del gestor de seguridad las procesa el servidor de sincronización.

La lista siguiente resume información adicional de seguridad que necesita saber para configurar el servidor de sincronización:

- Para que TADDM funcione correctamente, el portal de gestión de datos debe estar ejecutándose en el servidor de sincronización. Un dominio de TADDM delega operaciones de seguridad en el Portal de gestión de datos, y esta delegación se actualiza cada 2,5 minutos. Si pasan 5 minutos y esta delegación no se actualiza, el dominio de TADDM dejará de delegar operaciones de seguridad y continuará funcionando como si no hubiera ningún servidor de sincronización. En esta situación, deben reiniciarse las UI de TADDM para restablecer las sesiones con el servidor de sincronización.
- En cada una de las situaciones siguientes, la UI de TADDM debe reiniciarse para restablecer las sesiones con el servidor de sincronización correcto:
  - El dominio en el que se ejecuta la UI se añade al portal de gestión de datos en ejecución en el servidor de sincronización.
  - La UI se abre en un dominio mientras el dominio está conectado a un Portal de gestión de datos, pero el servidor de sincronización deja de estar disponible más tarde, como al reiniciar el servidor de sincronización o cuando se producen problemas de red.
- Los roles, permisos y las colecciones de accesos que se almacenan en el servidor de TADDM están sincronizados desde el dominio al servidor de sincronización. Las correlaciones de usuarios con roles no se sincronizan.
- Los roles creados para el dominio se pueden utilizar por el servidor de sincronización después de sincronizar estos objetos desde el dominio al servidor de sincronización.
- Los usuarios no se sincronizan con el servidor de sincronización.
- Un registro central de usuarios, como LDAP o un registro de repositorios federados de WebSphere, es el método preferido de autenticación para el servidor de sincronización. Utilizando un registro central de usuarios, las contraseñas de usuario se almacenan en una ubicación.
- Las colecciones de accesos no pueden abarcar dominios.
- La sincronización funciona desde el dominio al servidor de sincronización. Los objetos creados en el servidor de sincronización no se propagan al dominio.
- Cree y llene las colecciones de acceso en el dominio y sincronícelas con el servidor de sincronización.

- Cree roles en el dominio y sincronícelos con el servidor de sincronización.
- Autorice usuarios en el servidor de sincronización para otorgar acceso a las colecciones de accesos de varios dominios.

Seguridad para un despliegue de servidor de modalidad continua

Si utiliza un despliegue de servidor de modalidad continua, la autenticación y la autorización se delegan en el servidor de almacenamiento primario.

Si utiliza el registro basado en archivo de TADDM, debe crear y autorizar a los usuarios de TADDM en el servidor de almacenamiento primario. Si utiliza un Lightweight Directory Access Protocol (LDAP) o un registro de usuario de repositorios federados de WebSphere, debe autorizar a los usuarios de TADDM en el servidor de almacenamiento primario. El tipo de registro preferido para la autenticación de TADDM es uno con un registro de usuario central, como un registro LDAP o un registro de repositorio federado de WebSphere.

Los inicios de sesión a servidores de descubrimiento y servidores de almacenamiento secundario se procesan en el servidor de almacenamiento primario. Por lo tanto, se lleva a cabo la autenticación del usuario en el registro de usuarios para el que está configurado el servidor de almacenamiento primario. Además, las funciones del gestor de seguridad las procesa el servidor de almacenamiento primario.

Para que TADDM funcione correctamente, el servidor de almacenamiento primario debe estar en ejecución.

Si el servidor de almacenamiento primario se detiene o reinicia, debe reiniciarse la interfaz de usuario de TADDM para restablecer las sesiones con el servidor de almacenamiento primario.

Configuración de LDAP

Puede configurar un servidor LDAP externo para la autenticación de usuarios.

Antes de empezar

Si desea autenticarse con un registro de usuarios LDAP, configure un registro LDAP V2 o V3.

Acerca de esta tarea

Si se utiliza LDAP y/o VMM, los usuarios y/o grupos de LDAP siempre se almacenan en LDAP/VMM y no se tienen que crear en TADDM. TADDM se utiliza únicamente para asignar roles a los usuarios y grupos de LDAP. Solo estas correlaciones de usuario/grupo con rol, conocidos como permisos, tienen que crearse y almacenarse en TADDM. El ID de usuario administrador es un usuario TADDM interno especial que siempre se procesa mediante seguridad basada en archivos, sin importar qué registro de usuarios esté configurado. Este usuario siempre se puede utilizar para asignar roles inicialmente a los usuarios y grupos de LDAP.

Procedimiento

Para utilizar LDAP o VMM para la autenticación de usuario, complete los pasos siguientes:

1. Configure TADDM para utilizar el registro de LDAP mediante la configuración de las propiedades adecuadas en el archivo collation.properties.
2. Inicie sesión en el portal de gestión de datos mediante el ID de usuario administrador de TADDM.
3. Efectúe uno de los pasos siguientes:
   - En el panel Usuarios, utilice el campo **Buscar usuarios** para buscar el registro de LDAP para el usuario correspondiente.
   - En el panel Grupos de usuarios, utilice el campo **Buscar grupos** para buscar el registro de LDAP para el grupo de usuarios correspondiente.

   Nota: Los resultados de la búsqueda listan los nombres de usuarios o grupos devueltos por la búsqueda del registro LDAP. No se trata de un medio de crear usuarios ni de copiar usuarios de LDAP a TADDM. La finalidad de la lista es mostrar qué permisos de TADDM tienen que crearse para los usuarios.
4. Después de que se liste el usuario (o el grupo), asigne los roles de TADDM necesarios para ellos. Únicamente estos permisos, y no los usuarios (o grupos) de LDAP, se almacenan en TADDM.

Qué hacer a continuación

Para configurar SSL para LDAP, complete los pasos siguientes:

1. En el archivo `collation.properties`, localice la siguiente propiedad y cambie el valor de la propiedad de `false` a `true`:

   ```
   com.collation.security.auth.ldapUseSSL
   ```
2. Configure las siguientes propiedades del almacén de confianza y el almacén de claves según corresponda:

   ```
   com.collation.security.auth.ldapClientKeyStore
   com.collation.security.auth.ldapClientKeyStorePassphrase
   com.collation.security.auth.ldapClientTrustStore
   com.collation.security.auth.ldapClientTrustStorePassphrase
   ```
3. Si es necesario, cambie el puerto en el que el servidor LDAP escucha las conexiones SSL mediante la configuración de la siguiente propiedad:

   ```
   com.collation.security.auth.ldapPortNumber
   ```

Configuración de repositorios federados de WebSphere

Si dispone de una aplicación de Tivoli WebSphere configurada para un registro de usuarios centralizado que utiliza repositorios federados de WebSphere, puede configurar los repositorios federados de WebSphere en un registro de repositorios federados.

Configuración del servidor de TADDM para utilizar repositorios federados de WebSphere

Los repositorios federados de WebSphere están formados por un metarepositorio flexible, dentro de WebSphere, que da soporte a varios tipos de registros de usuarios, entre los que se incluye Microsoft Active Directory.

Antes de empezar

Debe configurar TADDM para que utilice los repositorios federados de WebSphere si utiliza otros productos de Tivoli en su entorno, entre los que se incluyen cualquiera de los productos siguientes:

- IBM Tivoli Change and Configuration Management Database (CCMDB) o IBM SmartCloud Control Desk (SCCD)
- IBM Tivoli Business Service Manager

TADDM requiere servicios adicionales no existentes en una distribución de WebSphere estándar, de modo que cuando configure TADDM para los repositorios federados, debe utilizar una de las siguientes instalaciones de WebSphere:

- WebSphere Application Server Network Deployment, según se instala con CCMDB o SCCD
- WebSphere Application Server, según se instala con IBM Tivoli Business Service Manager

Para ver las versiones soportadas de los productos, vaya a la sección "Versiones soportadas" en la página 200.

Antes de iniciar este procedimiento, debe tener configurado el servicio de autenticación de repositorios federados WebSphere en un servidor de WebSphere Application Server Network Deployment. Para obtener más información, consulte la documentación de IBM Tivoli Change and Configuration Management Database (CCMDB) o la documentación IBM de SmartCloud Control Desk (SCCD).

Acerca de esta tarea

Esta configuración permite efectuar un inicio de sesión único entre las aplicaciones de Tivoli, mediante las señales de WebSphere Lightweight Third-Party Authentication (LTPA). Por ejemplo, al configurar TADDM para utilizar los mismos repositorios federados de WebSphere que utiliza CCMDB o SCCD, se da soporte al inicio de sesión único para poder iniciar en contexto entre IBM Tivoli CCMDB o IBM SCCD y TADDM.

Para configurar automáticamente TADDM para utilizar los repositorios federados de WebSphere, instale TADDM y seleccione **Repositorios federados de WebSphere** como registro de usuario durante la instalación.

Esta configuración la soportan todos los tipos de servidor de TADDM en todos los despliegues

Procedimiento

Para llevar a cabo la configuración normalmente, realice los pasos siguientes:

1. Detenga el servidor de TADDM.
2. Especifique el módulo de gestión de usuario utilizado por el servidor de TADDM. Los valores siguientes son válidos:

   archivo
   Este valor se utiliza para un registro de usuarios basado en archivo. (Éste es el valor predeterminado.)

   ldap Este valor se utiliza para un registro de usuario de LDAP.

vmm Este valor se utiliza para un registro que utiliza repositorios federados de WebSphere Application Server.

Por ejemplo, en el archivo `$COLLATION_HOME/etc/collation.properties`:

```
com.collation.security.usermanagementmodule=vmm
```

3. Especifique el nombre de host y el puerto de WebSphere en el archivo `collation.properties`. Por ejemplo:

   ```
   com.collation.security.auth.websphereHost=localhost
   com.collation.security.auth.webspherePort=2809
   ```

   Cuando especifique el puerto de WebSphere en el archivo `collations.properties`, utilice la propiedad siguiente: `com.collation.security.auth.webspherePort`. El puerto WebSphere debe ser el puerto de la secuencia de arranque del servidor de WebSphere. Para WebSphere Application Server y la versión incorporada de WebSphere Application Server, el puerto predeterminado es 2809. Para WebSphere Application Server Network Deployment, que utiliza IBM Tivoli CCMDB o IBM SCCD, el puerto predeterminado es 9809.
4. Especifique el nombre de usuario y la contraseña de administrador de WebSphere en el archivo `collation.properties`. Por ejemplo:

   ```
   com.collation.security.auth.VMMAdminUsername=administrator
   com.collation.security.auth.VMMAdminPassword=password
   ```
5. Efectúe el cambio siguiente en el archivo de configuración de servicios de autenticación:
   - Para los sistemas operativos Linux, AIX y Linux en System z, el archivo se ubica en la siguiente vía de acceso: `$COLLATION_HOME/etc/ibmessclientauthncfg.properties`.
   - Para los sistemas operativos Windows, el archivo se encuentra en la vía de acceso siguiente: `%COLLATION_HOME%\etc\ibmessclientauthncfg.properties`.

   En la propiedad `authnServiceURL`, sustituya el nombre de dominio completo del sistema donde está instalada la instancia de WebSphere y el puerto HTTP de la instancia de WebSphere.

   ```
   # This is the URL for the Authentication Service
   authnServiceURL=http://localhost:9080/TokenService/services/Trust
   ```
6. Copie los archivos de WebSphere `orb.properties` y `iwsorbutil.jar` en el entorno JRE en el que esté instalado TADDM. Por ejemplo, en una instalación de TADDM bajo Linux, efectúe las acciones siguientes:
   a. Copie el archivo `dist/lib/websphere/6.1/orb.properties` a `dist/external/ jdk-Linux-i686/jre/lib/`.
   b. Copie el archivo `dist/lib/websphere/6.1/iwsorbutil.jar` a `dist/external/ jdk-Linux-i686/jre/lib/ext/`.
7. Especifique el nombre de host y el puerto de WebSphere en el archivo `sas.client.props`:
   - Para los sistemas operativos Linux, AIX y Linux en System z, el archivo se ubica en la siguiente vía de acceso: `$COLLATION_HOME/etc/sas.client.props`.
   - Para los sistemas operativos Windows, el archivo se encuentra en la vía de acceso siguiente: `%COLLATION_HOME%\etc\sas.client.props`, por ejemplo:

     ```
     com.ibm.CORBA.securityServerHost=host1.austin.ibm.com
     com.ibm.CORBA.securityServerPort=2809
     ```

   Nota: Para WebSphere Application Server y la versión incorporada de WebSphere Application Server, el puerto predeterminado es 2809. Para

WebSphere Application Server Network Deployment, que utiliza IBM Tivoli CCMDB o IBM SCCD, el puerto predeterminado es 9809.

8. Especifique el nombre de usuario y la contraseña del administrador de WebSphere en el archivo `sas.client.props`. Por ejemplo:

```
# RMI/IIOP user identity
com.ibm.CORBA.loginUserid=administrator
com.ibm.CORBA.loginPassword=password
```

9. Opcional: Para cifrar la contraseña de inicio de sesión en el archivo `sas.client.props`, efectúe los siguientes pasos:
   a. Copie el archivo `sas.client.props` de nuevo en el servidor de TADDM, en el directorio `$COLLATION_HOME/etc`.
   b. Cifre la contraseña tal como se indica a continuación, en función del sistema operativo en el que ha instalado WebSphere.
      - Para los sistemas operativos Linux, AIX y Linux en System z:

        Utilice el mandato `PropFilePasswordEncoder.sh`.
      - Para sistemas operativos Windows:

        Utilice `PropFilePasswordEncoder.bat`; por ejemplo,

```
C:\WebSphere\profiles\AppSrv01\bin\PropFilePasswordEncoder C:\temp\sas
  .client.props com.ibm.CORBA.loginPassword
```

   c. Copie el archivo `sas.client.props` de nuevo en el servidor de TADDM en el directorio `etc`.
10. Inicie el servidor de TADDM.

Qué hacer a continuación

Después de que finalice la instalación, puede utilizar el usuario administrador predeterminado definido en el repositorio basado en archivo de TADDM para configurar usuarios de TADDM adicionales, incluidos los administradores de TADDM. Estos usuarios adicionales de TADDM se autentican mediante los repositorios federados de WebSphere.

Existen configuraciones de seguridad para Tivoli CCMDB o IBM SCCD que permiten la creación y el mantenimiento de grupos y miembros de grupos en las aplicaciones de usuarios y grupos de Maximo.

Cuando Tivoli CCMDB o IBM SCCD se configura para esto, TADDM utiliza su propio repositorio independiente de Tivoli CCMDB o IBM SCCD. Los usuarios deben crearse en Tivoli CCMDB o IBM SCCD/Maximo y TADDM.

TADDM se puede configurar para utilizar las definiciones de usuario y grupo en los registros de usuarios externos a través de los repositorios federados de WebSphere. Sin embargo, TADDM no puede utilizar las definiciones de usuario y grupo que están almacenadas en Tivoli CCMDB porque éstas no las soportan los repositorios federados de WebSphere.

Actualización de claves de Lightweight Third Party Authentication (LTPA) de servicio de autenticación

Si se utiliza un inicio de sesión único con los repositorios federados de WebSphere se deben mantener sincronizadas las claves de Lightweight Third-Party Authentication (LTPA) del servicio de autenticación con las utilizadas por los repositorios federados de WebSphere.

Procedimiento

Si se cambian las claves de LTPA utilizadas por los repositorios federados de WebSphere, utilice este proceso para volver a sincronizar las claves utilizadas por el servicio de autenticación:

1. Exporte las nuevas claves de LTPA de WebSphere:
   a. En la consola administrativa de WebSphere, navegue hasta **Administración segura, aplicaciones e infraestructura** > **Mecanismos de autenticación y vencimiento**.
   b. En **Inicio de sesión único entre celdas**, especifique un nombre de archivo y una contraseña para el archivo que contiene las claves de Lightweight Third Party Authentication (LTPA).
2. En el indicador de mandatos, navegue hasta el directorio `bin` del perfil de WebSphere adecuado.
3. Ejecute el siguiente comando **wsadmin** de WebSphere:

   ```
   wsadmin> $AdminTask importESSLTPAKeys {-pathname vía_acceso -password contrase}
   ```

   donde *vía_acceso* y *contrase* son los valores que especifica el usuario para el nombre y la contraseña del archivo al exportar las claves de Lightweight Third Party Authentication (LTPA).
4. Reinicie el servidor de WebSphere.

Cómo asegurar el canal de autenticación

Cuando configure TADDM para que utilice los repositorios federados de WebSphere, puede asegurar las comunicaciones entre el cliente de autenticación y el servicio de autenticación.

Acerca de esta tarea

TADDM utiliza un servicio de autenticación que soporta el inicio de sesión único. El servicio de autenticación se instala durante la instalación de IBM Tivoli Change and Configuration Management Database (IBM SmartCloud Control Desk (SCCD)) o IBM Tivoli Business Service Manager.

Para ver las versiones soportadas de los productos, vaya a la sección “Versiones soportadas” en la página 200.

Existen dos mecanismos mediante los cuales puede garantizar las comunicaciones entre un cliente de autenticación y un servicio de autenticación:

- SSL
- Autenticación de cliente

Configuración del canal de autenticación para SSL:

Puede hacer que las comunicaciones sean seguras utilizando certificados de firmante de WebSphere para configurar SSL entre el cliente de autenticación y el servidor de autenticación.

Procedimiento

Para configurar para SSL entre el cliente de autenticación y el servidor de autenticación, efectúe los pasos siguientes:

1. Efectúe una de las acciones siguientes:

a. Si utiliza la instancia de WebSphere instalada por Tivoli Integrated Portal, navegue a **Certificado SSL y gestión de claves** > **Gestionar configuraciones de seguridad de punto final** > **Node1** > **Almacenamientos y certificados de claves** > **NodeDefaultTrustStore** > **Certificados de firmante**.

b. Si utiliza la instancia de WebSphere instalada por Tivoli Change and Configuration Management Database (CCMDB) o IBM SmartCloud Control Desk, navegue a **Certificado SSL y gestión de claves** > **Gestionar configuraciones de seguridad de puntos finales** > **ctgNode01** > **Almacenamientos y certificados de claves** > **NodeDefaultTrustStore** > **Certificados de firmante**.

2. Exporte los certificados de firmante de WebSphere a archivos (por ejemplo, exporte dummyclientsigner a `signer1.cert` y dummyserversigner a `signer2.cert`). Si no está seguro de los certificados que va a exportar, debe exportar todos los certificados de firmante.
3. Copie los archivos de extensión `.cert` al servidor de TADDM. Cree un almacén de confianza e importe los certificados de firmante de WebSphere tal como se indica a continuación:

```
$COLLATION_HOME/external/jdk-Linux-i686/jre/bin/keytool \
-genkey -alias truststore -keystore truststore.jks
$COLLATION_HOME/external/jdk-Linux-i686/jre/bin/keytool \
-import -trustcacerts -alias default -file signer1.cert -keystore truststore.jks
$COLLATION_HOME/external/jdk-Linux-i686/jre/bin/keytool \
-import -trustcacerts -alias dummyserversigner -file signer2.cert -keystore truststore.jks
```

4. Incluya la contraseña de almacén de confianza y la ubicación en las entradas de `$COLLATION_HOME/etc/collation.properties`:

```
com.collation.security.auth.ESSClientTrustStore=/opt/IBM/taddm/dist/etc/truststore.jks
com.collation.security.auth.ESSClientTrustPwd=contraseña
```

5. Actualice el localizador universal de recursos de Tivoli Authentication Service en el archivo `ibmessclientauthncfg.properties` para utilizar https y el puerto 9443. Asegúrese de que el nombre de host de WebSphere es correcto, sustituyéndolo por un sistema principal local, y que se comenta la entrada que no es de https.

```
# This is the URL for the ESS Authentication Service
#authnServiceURL=http://localhost:9080/TokenService/services/Trust
authnServiceURL=https://localhost:9443/TokenService/services/Trust
```

Configuración de la autenticación de cliente:

Para configurar la autenticación de cliente entre el cliente de autenticación y el servidor de autenticación, se recomienda que habilite la seguridad de la aplicación de WebSphere.

Antes de empezar

Después de habilitar la seguridad de la aplicación de WebSphere, puede añadir la función denominada TrustClientRole para el usuario administrador de WebSphere especificado durante la instalación de TADDM. Esto ofrece seguridad añadida para el servicio de autenticación limitando los usuarios que se pueden autenticar en el servicio de autenticación a únicamente aquellos que tienen TrustClientRole.

Procedimiento

Para añadir TrustClientRole al administrador de WebSphere especificado durante la instalación de TADDM, complete los siguientes pasos:

1. Inicie la sesión en WebSphere Administration Console.

2. En la pestaña **Seguridad**, pulse **Aplicaciones de empresa**. Se visualiza el panel Aplicaciones empresariales.
3. En la tabla Aplicaciones empresariales, pulse la aplicación Authentication Service (authnsvc_ctges) en la columna Nombre. Se visualiza el panel Aplicaciones empresariales > authnsvc_ctges.
4. En el panel Aplicaciones empresariales > authnsvc_ctges, en la lista Propiedades detalladas, pulse **Rol de seguridad para correlación de usuarios/grupos**. Se visualiza el panel Aplicaciones empresariales > authnsvc_ctges > Correlación de rol de seguridad con usuario/grupo.
5. En la tabla del panel Aplicaciones empresariales > authnsvc_ctges > Correlación de rol de seguridad con usuario/grupo siga estos pasos:
   - En la tabla, seleccione el recuadro de selección junto a TrustClientRole.
   - Borre el recuadro de selección **Todos**.
   - pulse **Buscar usuarios** o **Buscar grupos**. Se visualiza el panel Aplicaciones empresariales > authnsvc_ctges > Correlación de rol de seguridad con usuario/grupo > Buscar usuarios o grupos.
   - En el panel Aplicaciones empresariales > authnsvc_ctges > Correlación de rol de seguridad con usuario/grupo > Buscar usuarios o grupos, lleve a cabo los pasos siguientes:
     – Busque los usuarios o grupos, utilizando los recuadros Limitar y buscar entrada de serie. Cuando se encuentra un grupo o usuario, se visualiza en la lista Disponible.
     – En la lista Disponible, seleccione el usuario o grupo que desee.
     – pulse **Mover** para añadir el usuario o grupo a la lista **Seleccionado**.
   - Pulse **Aceptar**. Se visualiza el panel Aplicaciones empresariales > authnsvc_ctges > Correlación de rol de seguridad con usuario/grupo.
   - En el panel Aplicaciones empresariales > authnsvc_ctges > Correlación de rol de seguridad con usuario/grupo, borre la casilla de verificación **Todos**.
   - Pulse **Aceptar**. Se visualiza el panel Aplicaciones empresariales > authnsvc_ctges.
   - Pulse **Guardar** para guardar la configuración. Se visualiza el panel Aplicaciones empresariales.
   - Pulse **Aceptar**. Se visualiza el panel Aplicaciones empresariales > authnsvc_ctges.

Configuración de Microsoft Active Directory

Puede utilizar Microsoft Active Directory como método de autenticación para TADDM usando LDAP o los repositorios federados de WebSphere como intermediarios. Si necesita un inicio de sesión único en TADDM, debe utilizar repositorios federados de WebSphere.

Acerca de esta tarea

Puede utilizar los usuarios definidos en el registro de Active Directory, sin definir nuevos usuarios mediante la configuración de TADDM para utilizar Active Directory. Puede configurar TADDM para utilizar Active Directory como registro LDAP, o puede configurar TADDM para utilizar repositorios federados de WebSphere y, a continuación, configurar los repositorios federados de WebSphere para Active Directory.

Cuando configure Active Directory durante la instalación de TADDM, puede configurar TADDM para utilizar cualquier usuario de Active Directory como

administrador de TADDM. El administrador tiene permisos para configurar el acceso a TADDM y obtener otros acceso de usuario a objetos y servicios de TADDM.

Esta configuración la soportan todos los tipos de servidor de TADDM en todos los despliegues

Procedimiento

Para realizar la configuración de Microsoft Active Directory, complete los pasos siguientes:

Efectúe una de las acciones siguientes:

- Para configurar Microsoft Active Directory mediante LDAP:
  1. Configure TADDM para LDAP. Para obtener más información sobre configurar TADDM para LDAP, consulte "Configuración de LDAP" en la página 26.
  2. Asegúrese de que cuando utilice Active Directory, defina **com.collation.security.auth.ldapFollowReferrals** en *true* en el archivo `collation.properties`.
- Para configurar Microsoft Active Directory mediante los repositorios federados de WebSphere:
  1. Configure TADDM para repositorios federados de WebSphere. Para obtener más información sobre TADDM para repositorios federados de WebSphere, consulte "Configuración del servidor de TADDM para utilizar repositorios federados de WebSphere" en la página 27.
  2. Configure los repositorios federados de WebSphere para Microsoft Active Directory. Para obtener más información sobre los tipos de entidad soportados en la configuración de repositorios federados, consulte el apartado denominado **Configuring supported entity types in a federated repository configuration** (configuración de tipos de entidades soportadas en una configuración de repositorios federados) en *WebSphere Application Server Information Center*,http://www-01.ibm.com/support/knowledgecenter/SSAW57_6.1.0/com.ibm.websphere.nd.doc/info/ae/ae/twim_entitytypes.html.

Protección de los servicios web de TADDM

Puede configurar TADDM para inhabilitar el puerto HTTP estableciendo la propiedad `com.ibm.cdb.secure.tomcat` (TADDM 7.3.0) o la propiedad `com.ibm.cdb.secure.liberty` (TADDM 7.3.0.1 y posteriores) de `collation.properties` en `true`. Asimismo, puede establecer un protocolo SSL más seguro utilizando el distintivo `com.ibm.cdb.http.ssl.protocol`.

El valor predeterminado de las propiedades `com.ibm.cdb.secure.tomcat` y `com.ibm.cdb.secure.liberty` es `false`. Cuando el puerto HTTP está inhabilitado, sólo puede accederse a TADDM utilizando el puerto HTTPS, por ejemplo, `https://example.com:9431`.

Limitación: Cuando haya instalado TADDM en el despliegue del servidor en modalidad continua y estén activos y en ejecución los servidores de descubrimiento y los servidores de almacenamiento secundarios, puede establecer la propiedad `com.ibm.cdb.secure.tomcat` o `com.ibm.cdb.secure.liberty` en `true`. En este caso, el puerto HTTP está inhabilitado y puede utilizar TADDM en la modalidad segura. Sin embargo, si desea añadir un nuevo servidor de

descubrimiento o un servidor de almacenamiento secundario para su desarrollo, debe habilitar temporalmente el puerto HTTP, ya que el instalador de TADDM no da soporte al protocolo HTTPS. Para inhabilitar temporalmente la modalidad segura, realice estos pasos:

1. Cambie el valor de la propiedad `com.ibm.cdb.secure.tomcat` o `com.ibm.cdb.secure.liberty` a `false`.
2. Reinicie el servidor de TADDM.
3. Instale el nuevo servidor de descubrimiento o el servidor de almacenamiento secundario.
4. Cambie el valor de la propiedad `com.ibm.cdb.secure.tomcat` o `com.ibm.cdb.secure.liberty` a `true`.
5. Reinicie el servidor de TADDM.

El valor predeterminado de la propiedad `com.ibm.cdb.http.ssl.protocol` es `TLS`. Los valores seguros son `TLS`, `TLSv1.1` y `TLSv1.2`. Si desea utilizar los protocolos más seguros `TLSv1.1` y `TLSv1.2`, primero debe configurar el navegador web para darles soporte.

Instalación de certificados SSL personalizados para utilizarlos en TADDM

Puede instalar sus propios certificados SSL personalizados y utilizarlos con TADDM.

Procedimiento

1. Cree una copia de seguridad de los archivos de almacén de claves siguientes:
   - `$COLLATION_HOME/etc/serverkeys`
   - `$COLLATION_HOME/etc/jssecacerts.cert`
2. Vaya al directorio `$COLLATION_HOME/etc`, abra la línea de mandatos y especifique los parámetros `keytool` y `sslpassphrase` de TADDM con los valores de la siguiente forma:
   - Sistema operativo Linux:

     ```
     keytool=../external/jdk-Linux-x86_64/bin/keytool
     pass=XXXXXXXX30374
     ```

   - Sistema operativo Windows:

     ```
     set keytool=..\external\jdk-Windows-i386-64\bin\keytool.exe
     set pass=XXXXXXXX30374
     ```

   El valor del parámetro `pass` es el valor de la propiedad `com.collation.sslpassphrase` especificada en el archivo `collation.properties`.
3. Elimine el certificado autofirmado y la clave de TADDM ejecutando los mandatos siguientes:
   - Sistema operativo Linux:

     ```
     $keytool -delete -alias collation -noprompt -keystore jssecacerts.cert
     -storepass $pass
     $keytool -delete -alias collation -noprompt -keystore serverkeys -storepass
     $pass
     ```

   - Sistema operativo Windows:

     ```
     %keytool% -delete -alias collation -noprompt -keystore jssecacerts.cert
     -storepass %pass%
     %keytool% -delete -alias collation -noprompt -keystore serverkeys -storepass
     %pass%
     ```

4. Genere la clave SSL con el CN necesario, la validez, el algoritmo y otros parámetros, y guárdela en el archivo serverkeys. Por ejemplo, puede ejecutar el mandato siguiente:
   - Sistema operativo Linux:

     ```
     $keytool -genkey -alias collation -keystore serverkeys -validity 3650
     -keyAlg RSA -sigalg SHA256WithRSA -keypass $pass -storepass $pass -dname
     "CN=John Public, OU=Engineering, OU=NA, o=Company, L=Manhattan,
     S=New York, c=US"
     ```

   - Sistema operativo Windows:

     ```
     %keytool% -genkey -alias collation -keystore serverkeys -validity 3650
     -keyAlg RSA -sigalg SHA256WithRSA -keypass %pass% -storepass %pass% -dname
     "CN=John Public, OU=Engineering, OU=NA, o=Company, L=Manhattan,
     S=New York, c=US"
     ```

5. Cree otra copia de seguridad del archivo serverkeys, donde ha guardado la clave SSL generada.
6. Genere la solicitud de firma de certificado (archivo CSR) ejecutando el mandato siguiente:
   - Sistema operativo Linux:

     ```
     $keytool -certreq -alias collation -storepass $pass -file
     /tmp/certreq.csr -keystore serverkeys
     ```

   - Sistema operativo Windows:

     ```
     %keytool% -certreq -alias collation -storepass %pass% -file
     C:\temp\certreq.csr -keystore serverkeys
     ```

7. Utilice el archivo CSR para obtener el certificado SSL de la entidad emisora de certificados oficial. Guarde el certificado en el servidor de TADDM, por ejemplo en el directorio tmp del sistema operativo Linux, o en el directorio C:\temp del sistema operativo Windows como el archivo cert.crt.
8. Importe el certificado generado a TADDM, tanto para el archivo serverkeys como para el archivo jssecacerts.cert ejecutando los mandatos siguientes:

   Importante: Para el parámetro -file, especifique la vía de acceso al archivo donde ha guardado el certificado SSL en el paso anterior, por ejemplo /tmp/cert.crt en el sistema operativo Linux, o C:\temp\cert.crt en el sistema operativo Windows.
   - Sistema operativo Linux:

     ```
     $keytool -import -trustcacerts -alias collation -noprompt -keystore
     serverkeys -storepass $pass -keypass $pass -file /tmp/cert.crt
     $keytool -import -trustcacerts -alias collation -noprompt -keystore
     jssecacerts.cert -storepass $pass -keypass $pass -file /tmp/cert.crt
     ```

   - Sistema operativo Windows:

     ```
     %keytool% -import -trustcacerts -alias collation -noprompt -keystore
     serverkeys -storepass %pass% -keypass %pass% -file C:\temp\cert.crt
     %keytool% -import -trustcacerts -alias collation -noprompt -keystore
     jssecacerts.cert -storepass %pass% -keypass %pass% -file C:\temp\cert.crt
     ```

9. Reinicie el servidor de TADDM.

Qué hacer a continuación

Guarde las copias de seguridad del archivo serverkeys que ha generado en el paso 4, y el archivo donde ha guardado el certificado SSL en el paso 7. Si debe sustituir o renovar el certificado, son necesarios estos archivos. Para sustituir o renovar el certificado, complete los pasos siguientes:

1. Repita los pasos 2 y 3.
2. Restaure el archivo serverkeys.

3. Repita los pasos 8 y 9.

Gestión de servidores de TADDM

Antes de configurar TADDM para el descubrimiento, debe comprender cómo gestionar los servidores de TADDM, que incluye muchas tareas.

Comprobación del estado del servidor TADDM

Puede utilizar la consola del administrador o el mandato **control** para comprobar el estado del servidor de TADDM.

Utilización de la consola del administrador para comprobar el estado

Para utilizar la consola del administrador para comprobar el estado, abra un navegador web y especifique el URL y el número de puerto del sistema en el que ha instalado el servidor de TADDM. El siguiente URL es un ejemplo:

```
http://sistema.empresa.com:9430
```

Se muestra la consola del administrador donde se listan los componentes del servidor de TADDM y sus estados.

Utilización del mandato control para comprobar el estado

Para utilizar el mandato **control** para comprobar el estado del servidor, siga estos pasos:

1. Inicie la sesión como usuario no raíz que se ha definido durante el proceso de instalación.
2. En un indicador de mandatos, vaya al directorio en el que instaló el servidor de TADDM.
3. Ejecute uno de los mandatos siguientes:
   - Para los sistemas operativos AIX, Linux y Linux en System z:

     ```
     $COLLATION_HOME/bin/control status
     ```

   - Para sistemas operativos Windows:

     ```
     %COLLATION_HOME%\bin\control.bat status
     ```

   Se muestra la salida siguiente, en función del despliegue que tenga y del tipo de servidor en el que se está ejecutando TADDM en cada despliegue:

   despliegue del servidor de sincronización

   servidor de sincronización

   - TADDM 7.3.0:

     ```
     DbInit: Started
     Tomcat: Started
     EcmdbCore: Started

     TADDM: Running
     ```

   - TADDM 7.3.0.1 y posterior:

     ```
     DbInit: Started
     Liberty: Started
     EcmdbCore: Started

     TADDM: Running
     ```

   servidor del dominio

- TADDM 7.3.0:

```
Discover: Started
DbInit: Started
Tomcat: Started
Topology: Started
DiscoverAdmin: Started
Proxy: Started
EventsCore: Started

TADDM: Running
```

- TADDM 7.3.0.1 y posterior:

```
Discover: Started
DbInit: Started
Liberty: Started
Topology: Started
DiscoverAdmin: Started
Proxy: Started
EventsCore: Started

TADDM: Running
```

despliegue del servidor de modalidad continua

servidor de almacenamiento

- TADDM 7.3.0:

```
TADDM: Starting
EtaddmCore: Started
DbInit: Started
Tomcat: Started

TADDM: Running
```

- TADDM 7.3.0.1 y posterior:

```
TADDM: Starting
EtaddmCore: Started
DbInit: Started
Liberty: Started

TADDM: Running
```

servidor de descubrimiento

- TADDM 7.3.0:

```
Discover: Started
Tomcat: Started
DiscoverAdmin: Started
ProxyLite: Started
EventsCore: Started

TADDM: Running
```

- TADDM 7.3.0.1 y posterior:

```
Discover: Started
Liberty: Started
DiscoverAdmin: Started
ProxyLite: Started
EventsCore: Started

TADDM: Running
```

Inicio del servidor de TADDM

Si elige la opción **Iniciar al arrancar** en la instalación, el servidor de TADDM se inicia automáticamente durante cada arranque del sistema.

Acerca de esta tarea

Importante: Un servidor de base de datos remoto o local debe haberse iniciado y estar en ejecución antes de iniciar el servidor de TADDM. El servidor de TADDM no podrá inicializarse o ejecutarse debidamente si la base de datos no está disponible.

Procedimiento

Para iniciar manualmente el servidor de TADDM, efectúe los pasos siguientes:

1. Inicie la sesión como usuario no raíz que se ha definido durante el proceso de instalación.
2. Abra una ventana de indicador de mandatos.

   Nota: En un sistema Windows Server 2008 en el que se haya activado el Control de cuentas de usuario, abra la ventana de indicador de mandatos con privilegios de administrador. Para ello, pulse con el botón derecho del ratón en el icono Símbolo del sistema y, a continuación, pulse **Ejecutar como administrador**.
3. Vaya al directorio en el que instaló el servidor de TADDM.
4. Utilice uno de los mandatos siguientes para ejecutar el script de inicio:
   - Para los sistemas operativos Linux, AIX y Linux en System z:

     ```
     $COLLATION_HOME/bin/control start
     ```
   - Para sistemas operativos Windows:

     ```
     %COLLATION_HOME%\bin\startServer.bat
     ```

   Al iniciar el servidor en un sistema Windows, es posible que aparezca un mensaje de error de tiempo de espera excedido parecido al siguiente: `Error 1053: El servicio no ha respondido a la solicitud de inicio o de control en un período de tiempo apropiado.` Este error se genera porque el servidor de TADDM puede tardar más tiempo en iniciarse que el tiempo permitido. Puede ignorar este mensaje; el proceso de inicio continúa hasta que se completa.

   Si ha instalado el servidor de TADDM con privilegios de usuario root, puede iniciar manualmente el servidor de TADDM ejecutando el script siguiente:

   ```
   /etc/init.d/collation start
   ```

Detención del servidor de TADDM

Puede detener manualmente el servidor de TADDM y los procesos de descubrimiento relacionados.

Procedimiento

Para detener manualmente el servidor de TADDM, efectúe los pasos siguientes:

1. Inicie la sesión como usuario no raíz que se ha definido durante el proceso de instalación.
2. Abra una ventana de indicador de mandatos.

   Nota: En un sistema Windows Server 2008 en el que se haya activado el Control de cuentas de usuario, abra la ventana de indicador de mandatos con privilegios de administrador. Para ello, pulse con el botón derecho del ratón en el icono Símbolo del sistema y, a continuación, pulse **Ejecutar como administrador**.

3. Vaya al directorio en el que instaló el servidor de TADDM.
4. Utilice uno de los mandatos siguientes para ejecutar el script de detención:
   - Para los sistemas operativos Linux, AIX y Linux en System z:
     ```
     $COLLATION_HOME/bin/control stop
     ```
   - Para sistemas operativos Windows:
     ```
     %COLLATION_HOME%\bin\stopServer.bat
     ```

   Si ha instalado el servidor de TADDM con privilegios de usuario root, puede detener manualmente el servidor de TADDM ejecutando el script siguiente:
   ```
   /etc/init.d/collation stop
   ```

Qué hacer a continuación

Algunos sensores se ejecutan en su propia máquina virtual Java (JVM) especial. Cuando ejecute un descubrimiento, si utiliza el script de control (`./control stop`) para detener TADDM, es posible que necesite detener manualmente estas JVM adicionales, que se denominan anclas locales. Si no detiene las anclas locales, se puede producir un comportamiento imprevisto. Por ejemplo, es posible que el rendimiento de determinados descubrimientos disminuya.

Para verificar si el proceso del ancla local ya no se ejecuta, entre el mandato siguiente:

```
% ps -ef |grep -i anchor
```

Este mandato identifica los procesos de ancla local que se están ejecutando. La salida es similar al ejemplo de código siguiente:

```
coll   23751  0.0  0.0  6136  428 ?   S  Jun02   0:00 /bin/sh
   local-anchor.sh 8494 <más información aquí>
```

Si se ejecuta un proceso, detenga el proceso ejecutando el mandato siguiente:

```
-  % kill -9 23751
```

Tras ejecutar el mandato, verifique si se ha detenido el proceso ejecutando el mandato siguiente:

```
 % ps -ef |grep -i anchor
```

Copia de seguridad de datos

Copie los datos de forma regular para que se pueda recuperar de una anomalía del sistema.

Antes de empezar

Para poder realizar una copia de seguridad de los datos, es preciso que detenga el servidor de TADDM.

Procedimiento

Para realizar una copia de seguridad de los archivos para el servidor de TADDM, efectúe las tareas siguientes:

Guarde todos los archivos en el directorio en el que tenga instalado el servidor de TADDM.

- Para los sistemas operativos Linux, AIX y Linux en System z, la vía de acceso predeterminada al directorio es `/opt/IBM`.

- Para sistemas operativos Windows, la vía de acceso predeterminada al directorio es `C:\opt\IBM`.

Qué hacer a continuación

Para realizar copias de seguridad de los archivos de bases de datos, utilice la documentación que suministra el proveedor de la base de datos.

Restauración de datos

Tras una anomalía del sistema, podrá restaurar los datos de configuración y los archivos de la base de datos. Como consecuencia de ello, podrá reanudar el funcionamiento a partir de la última copia de seguridad realizada antes de producirse la anomalía.

Procedimiento

Para restaurar datos a partir de un soporte de copia de seguridad, efectúe los pasos siguientes:

1. Realice una de las acciones siguientes:
   - Restaure el directorio `/opt/IBM`, y reinicie TADDM.
   - Restaure el directorio `C:\opt\IBM`, y reinicie TADDM.
2. Localice la copia de seguridad de los archivos de datos.
3. Abra una ventana de indicador de mandatos.
4. Vaya al directorio en el que instaló el servidor de TADDM.
5. Copie la copia de seguridad de los archivos de datos en el directorio de instalación.
6. Cierre la ventana de indicador de mandatos.
7. Inicie el servidor de TADDM.

Qué hacer a continuación

Si la base de datos se ve afectada por la anomalía del sistema, restaure los archivos de base de datos utilizando la documentación del proveedor de base de datos.

Copia de ámbitos, perfiles y plantillas de servidores de descubrimiento entre servidores de TADDM

Puede utilizar el mandato **`datamover.sh|bat`** para copiar los ámbitos, perfiles de descubrimiento y plantillas del servidor personalizadas del descubrimiento entre servidores de TADDM.

Puede exportar los ámbitos, perfiles y plantillas de servidores personalizadas (todas las entidades) de descubrimiento o especificar qué entidad se va a exportar desde un servidor. A continuación, se puede importar la entidad o las entidades al servidor de destino.

Restricción: Para mantener la integridad de los datos, se deben transferir los datos entre las mismas versiones de servidores de TADDM.

Para copiar las entidades entre servidores de TADDM, efectúe los siguientes pasos:

1. Ejecute el siguiente mandato en el servidor de origen para exportar la entidad o las entidades a un archivo:

```
datamover.sh|bat -u usuario -p contraseña -a acción
[-t tipo ] [-f nombre_archivo]
```

donde:

usuario
Nombre de usuario de TADDM.

contraseña
Contraseña de usuario de TADDM.

acción
Especifique una de las siguientes acciones: `import`, `export`, o `help`.

Opcional: *tipo*
Especifique una de las siguientes acciones: `all`, `scope`, `profile`, `template`. El valor predeterminado es `all`.

Opcional: *nombre de archivo*
Especifique un nombre de archivo. El valor predeterminado es `datamover.xml`.

Los perfiles de descubrimiento predeterminados no se exportan, mientras que todas las plantillas de servidor personalizadas, los perfiles creados por el usuario y los ámbitos pueden exportarse.

Después de ejecutar el mandato, se muestra información acerca de las entidades exportadas. Por ejemplo, si el archivo de salida es `exporthost.xml`, se muestra la siguiente información:

```
Se han exportado 6 ámbitos
Se ha exportado 1 perfil
Se han exportado 57 plantillas
```

2. Copie el archivo o los archivos en el servidor de destino y ejecute **datamover.sh|bat** e importe la entidad o entidades.

   Cuando se importan las entidades se aplican las siguientes reglas:

   - Si existe un ámbito o perfil con el mismo nombre en el servidor, se renombra el ámbito o perfil importado. El archivo se renombra a *nombre*_TADDM.
   - Si existe una plantilla con el mismo nombre en el servidor, ésta se fusiona con la plantilla existente.

Despliegue de la consola de Discovery Management

Después de confirmar que el servidor de TADDM está disponible, puede desplegar la consola de Discovery Management.

Procedimiento

Para desplegar la consola de Discovery Management, efectúe los pasos siguientes:

1. Proporcione a los usuarios el URL (incluido el número de puerto) del sistema en el que ha instalado el servidor de TADDM.

   Por ejemplo, puede proporcionar a los usuarios un URL similar al siguiente:

   `http://sistema.empresa.com:9430`

2. Proporcione a los usuarios el nombre de usuario y la contraseña.
3. Especifique si los usuarios deben utilizar Secure Sockets Layer (SSL).

   En los casos en los que se utiliza SSL, enseñe a los usuarios a guardar un almacén de confianza para el servidor de TADDM siguiendo las instrucciones

que encontrará en la página de instalación e inicio de la consola de Discovery Management. Para obtener más información, consulte la *Guía de instalación* de TADDM.

Importante: Debe utilizar SSL en todas las comunicaciones entre la consola de Discovery Management y el servidor de TADDM.

4. Los usuarios deben tener una versión soportada del entorno de tiempo de ejecución Java instalada en el sistema que se utiliza para visualizar la consola de Discovery Management. Para obtener más información sobre los requisitos previos de cliente, consulte la *Guía de instalación* de TADDM .
5. Dirija a los usuarios a la *Guía del usuario* de TADDM de TADDM para obtener información sobre cómo iniciar la consola de Discovery Management.

Configuración de la comunicación de TADDM

Para establecer la comunicación de TADDM, es necesario configurar todos los servicios, las conexiones y los cortafuegos que sean necesarios.

Servicios de TADDM

La conectividad de TADDM se puede dividir en tres áreas:

Conectividad pública
La conectividad pública abarca la conectividad de red que se realiza desde el exterior de la infraestructura de TADDM. Por ejemplo, el portal de gestión de datos, la consola de Discovery Management o los clientes API, que se conectan al servidor de TADDM. Se trata del nivel de conectividad más elevado.

Conectividad entre servidores
La conectividad entre servidores abarca la conectividad de red entre elementos de la infraestructura principal de TADDM; es decir, los servidores de descubrimiento y los servidores de almacenamiento. Se trata del nivel de conectividad medio.

Conectividad local
La conectividad local abarca la conectividad de red entre servicios locales de una sola máquina. Se trata del nivel de conectividad más bajo.

La conectividad para cada servicio se puede configurar durante la fase de instalación o más adelante, mediante el cambio de las propiedades de configuración en el archivo de configuración `collation.properties`.

Interfaz predeterminada de servicios
Para configurar la interfaz de escucha predeterminada de servicios, cambie la propiedad `com.ibm.cdb.global.hostname` en el archivo `collation.properties`.

Tabla 2. Valores de la interfaz predeterminada de servicios

Nombre	Propiedad de configuración	Interfaz predeterminada
Host de Global Services	com.ibm.cdb.global.hostname	0.0.0.0

Interfaz de a que depende del tipo de comunicación
Para configurar las interfaces de escucha por separado para los servicios de cada área de conectividad, cambie la propiedad correspondiente en el archivo `collation.properties`.

Tabla 3. Valores de la interfaz predeterminada de servicios

Nombre	Propiedad de configuración	Interfaz predeterminada
Host de servicios de conectividad pública	com.ibm.cdb.public.hostname	Definido por com.ibm.cdb.global.hostname
Host de servicios de conectividad entre servidores	com.ibm.cdb.interserver.hostname	Definido por com.ibm.cdb.global.hostname
Host de servicios de conectividad local	com.ibm.cdb.local.hostname	127.0.0.1

Nota: Si no se ha especificado ninguna interfaz o la interfaz tiene el valor `0.0.0.0.`, debe abrirse una interfaz de red externa local para comunicarse con ella misma. Si se ha especificado una interfaz, debe abrirse para comunicarse con ella misma.

Interfaz de escucha para servicios específicos

Puede configurar el puerto TCP correspondiente para cada servicio durante la fase de instalación o más adelante, mediante el cambio de la propiedad respectiva en el archivo `collation.properties`.

Configuración de las interfaces de servicio

Para configurar una interfaz de escucha específica para cada servicio, cambie la propiedad correspondiente con el sufijo `host` en el archivo `collation.properties`.

Ejemplo para el servicio TopologyManager:

```
com.ibm.cdb.service.TopologyManager.host=192.168.1.5
```

Nota: Esta convenio de denominación no se aplica a los registros de servicio público o entre servidores.

Configuración de los puertos de servicio

Para configurar un puerto de escucha específico para cada servicio, cambie la propiedad correspondiente con el sufijo `port` en el archivo `collation.properties`.

El ejemplo siguiente corresponde al servicio TopologyManager:

```
com.ibm.cdb.service.TopologyManager.port=9550
```

Configuración del servicio SSL

Para configurar una interfaz o un puerto de escucha específico para cada servicio SSL, cambie la propiedad correspondiente con el infijo `secure` en el archivo `collation.properties`.

El ejemplo siguiente corresponde al servicio SecureApiServer:

- `com.ibm.cdb.service.SecureApiServer.secure.host=192.168.1.5`
- `com.ibm.cdb.service.SecureApiServer.secure.port=9531`

Configuración de la interfaz del portal web (HTTP y HTTPS)

Para configurar una interfaz de escucha para el portal web (HTTP y HTTPS), cambie la propiedad `com.ibm.cdb.service.web.host` en el archivo `collation.properties`.

Nota: El host HTTP y HTTPS se configura mediante el cambio de una sola propiedad, a diferencia de lo que sucede con otros servicios.

Conexiones de base de datos

Para configurar una conexión de base de datos específica, cambie las propiedades `com.collation.db.port` y `com.collation.db.server` en el archivo `collation.properties`.

Por ejemplo:

- `com.collation.db.port=65432`
- `com.collation.db.server=9.156.47.156`

Conexiones DNS

Si desea utilizar nombres de dominio completos (FQDN) para la comunicación, asegúrese de que el host que participa en la comunicación puede resolver el FQDN desde el servicio DNS.

Conexiones de sensor

La configuración de los puertos que utilizan el sensor de ping y el sensor de puertos para realizar conexiones se incluye en las documentaciones de dichos sensor de ping y sensor de puertos. Asegúrese de que los puertos para los servicios que desea descubrir están abiertos.

Tabla 4. Puertos predeterminados del sensor de ping y el sensor de puertos

Nombre de puerto	Puerto predeterminado	Protocolo
SSH	22	TCP
Telnet	23	TCP
DNS	53	TCP
WMI	135	TCP
Fix Pack 2 PowerShell	5985, 5986	TCP
LDAP	389	TCP
SMB	445	TCP
Oracle	1521	TCP
CiscoWorks	1741	TCP

Conexiones de ancla

TADDM puede conectarse a un servidor ancla mediante cualquiera de los siguientes tipos de conexión: *ssh* o *direct*. Para configurar un tipo de conexión de ancla específico, cambie el valor de la propiedad `com.collation.discover.anchor.connectType` en el archivo `collation.properties` a *ssh* o *direct*.

Para configurar un tipo de conexión de ancla específico para una dirección concreta, cambie la propiedad `com.collation.discover.anchor.connectType` con la dirección IP como sufijo en el archivo `collation.properties`; por ejemplo:

`com.collation.discover.anchor.connectType.1.2.3.4=`*`direct`*

Además, el puerto 8497 está definido como el puerto predeterminado para la conexión a un servidor ancla. Este puerto se puede configurar mediante la consola de Discovery Management.

- En la modalidad *ssh*, abra puertos para comunicación SSH en la interfaz pública a la que se accede desde el servidor de TADDM y desde el puerto de conexión de ancla en la interfaz de bucle de retorno de la máquina que aloja el servidor ancla.
- En la modalidad *direct*, abra puertos para comunicación SSH y conexión de ancla en la interfaz pública a la que se accede desde el servidor de TADDM.

Conexiones de pasarela

TADDM puede conectarse a un servidor de pasarela mediante una conexión SSH.

En la pasarela, el puerto SSH del host debe estar abierto para comunicación en una interfaz pública a la que se accede desde el servidor de TADDM.

Resolución de un nombre de host de servidor en un nombre de dominio totalmente calificado

Para asegurarse de que la comunicación entre los servidores se realiza correctamente, el servidor del host debe poder resolver su nombre de host en un nombre de dominio totalmente calificado (FQDN) utilizando la biblioteca resolver del sistema operativo. Se debe cumplir una de las condiciones siguientes:

- En el orden de búsqueda de la resolución de host del sistema operativo, el DNS debe preceder a los archivos locales. Para configurar este valor, consulte la documentación del sistema operativo.
- En el archivo de host, el FQDN del servidor TADDM debe preceder al nombre abreviado.

Si no se cumple ninguna de estas condiciones, puede establecer la propiedad `com.collation.serverID` del archivo `collation.properties` en la IP o nombre de host del servidor TADDM. Asimismo, asegúrese de que el ID de servidor del servidor de sincronización / Enterprise Server > Data Management Portal > Gestión de dominios > Nombre de host del dominio se haya establecido en el mismo valor.

Puertos temporales

La comunicación de TADDM incluye el uso de puertos temporales. Dichos puertos son específicos para cada sistema operativo. Cada sistema operativo tiene un rango de números de puerto desde el cual se eligen los puertos al azar. El TADDM no define estos puertos. Para obtener información sobre el rango de puertos, la configuración necesaria y más detalles, consulte la documentación del sistema operación que utiliza.

Configuración de cortafuegos

Para establecer la comunicación de TADDM, es necesario configurar los cortafuegos necesarios. Los detalles de esta tarea varían en función de si se ha

configurado un despliegue de servidor de dominio, un despliegue de servidor de modalidad continua o un despliegue de servidor de sincronización.

La información sobre la configuración del cortafuegos se presenta en tablas. Cada tabla incluye la dirección de la comunicación. En la máquina de destino, el puerto de servicio de destino debe estar abierto en el cortafuegos como el origen de las conexiones salientes y como el destino de las conexiones entrantes. En la máquina de origen, el puerto de servicio de destino debe estar abierto en el cortafuegos como el destino de las conexiones salientes y como el origen de las conexiones entrantes.

Importante: Los servicios de nivel superior también deben estar disponibles desde clientes de bajo nivel. Por ejemplo, los servicios públicos también deben estar abiertos para conectividad entre servidores.

Si la dirección especificada en la tabla se describe como de bucle de retorno, toda comunicación debe estar abierta en esta interfaz. Si cambia cualquier configuración de puertos predeterminada, asegúrese de abrir los puertos que sean apropiados para la configuración de su entorno.

Configuración de cortafuegos en un despliegue de servidor de dominio

Es necesario configurar los cortafuegos en un despliegue de servidor de dominio de manera que algunos puertos específicos estén abierto para comunicación.

La figura siguiente muestra comunicación de TADDM en un despliegue de servidor de dominio.

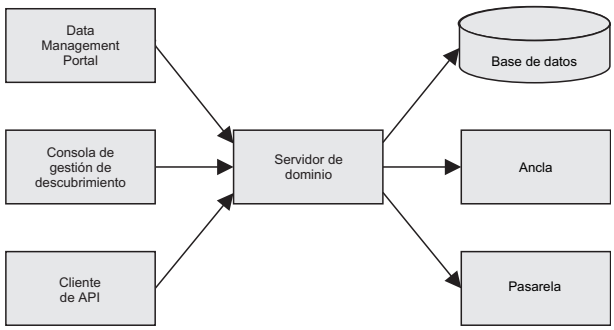

Figura 1. Comunicación de TADDM en un despliegue de servidor de dominio

Servicios de conectividad:

Para el despliegue de un servidor de dominio, puede configurar servicios de conectividad pública, entre servidores y local.

Servicios de conectividad pública

La tabla siguiente muestra los valores de host predeterminados para los servicios de conectividad pública del servidor de dominio.

Tabla 5. Valores de host predeterminados para los servicios de conectividad pública del servidor de dominio

Nombre	Propiedad de configuración	Interfaz predeterminada
Host de servicio público	com.ibm.cdb.public.hostname	Definido por com.ibm.cdb.global.hostname

La tabla siguiente muestra los valores de puerto predeterminados para servicios de conectividad pública del servidor de dominio.

Tabla 6. Valores de puerto predeterminados para los servicios de conectividad pública del servidor de dominio

Nombre	Propiedad de configuración	Protocolo	Puerto predeterminado
Puerto del servidor de la API	com.ibm.cdb.service.ApiServer.port	TCP	9530
Puerto de servidor de API seguro	com.ibm.cdb.service.SecureApiServer.secure.port	TCP	9531
Puerto HTTP (sin SSL)	com.ibm.cdb.service.web.port	TCP	9430
Puerto HTTPS (con SSL)	com.ibm.cdb.service.web.secure.port	TCP	9431
Puerto de comunicación del servidor de la GUI	com.ibm.cdb.service.ClientProxyServer.port	TCP	9435
Puerto de comunicación SSL del servidor de la GUI	com.ibm.cdb.service.SecureClientProxyServer.secure.port	TCP	9434
Puerto de registro de servicio público	com.ibm.cdb.service.registry.public.port	TCP	9433

Servicios de conectividad local

Los puertos de servicios locales no están definidos de forma explícita. Todos los puertos tienen que estar abiertos en la interfaz que esté definida para servicios locales. La interfaz predeterminada es el bucle de retorno.

La tabla siguiente muestra los valores de host predeterminados para los servicios de conectividad local del servidor de dominio.

Tabla 7. Valores de host predeterminados para los servicios de conectividad local del servidor de dominio

Nombre	Propiedad de configuración	Interfaz predeterminada
Host de servicio local	com.ibm.cdb.local.hostname	127.0.0.1

Configuración de la comunicación en el despliegue de servidor de dominio:

Para establecer correctamente la comunicación en el despliegue del servidor de dominio, configure los servicios de conectividad públicos y locales.

En las siguientes tablas se muestran los elementos que puede conectar en el despliegue del servidor de dominio y los puertos que debe abrir para que la comunicación se establezca correctamente.

Comunicación entre el servidor de base de datos y el servidor de dominio

Tabla 8. Comunicación entre el servidor de base de datos y el servidor de dominio.

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración
Servidor de bases de datos	5000	←	Servidor de dominio	

Comunicación entre el portal de gestión de descubrimiento; los clientes de API y los clientes del portal web y de Data Management Portal; y el servidor de

dominio

Tabla 9. Comunicación entre el portal de gestión de descubrimiento; los clientes de API y los clientes de Data Management Portal; y el servidor de dominio.

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración
Portal de gestión de descubrimiento	9433	→	Servidor de dominio - Registro de servicio público	com.ibm.cdb.service.registry.public.port
	9435	→	Servidor de dominio - ClientProxyServer	com.ibm.cdb.service.ClientProxyServer.puerto
	9434	→	Servidor de dominio - SecureClientProxyServer	com.ibm.cdb.service.SecureClientProxyServer.secure.port
Clientes de API	9433	→	Servidor de dominio - Registro de servicio público	com.ibm.cdb.service.registry.public.port
	9530	→	Servidor de dominio - Servidor de API	com.ibm.cdb.service.ApiServer.port
	9531	→	Servidor de dominio - Servidor de API seguro	com.ibm.cdb.service.SecureApiServer.secure.port
Clientes del portal web y de Data Management Portal	9430	→	Servidor de dominio - Web	com.ibm.cdb.service.web.port
	9431	→	Servidor de dominio - Web segura	com.ibm.cdb.service.web.secure.port

Comunicación entre el ancla y la pasarela y el servidor de dominio

Tabla 10. Comunicación entre el ancla y la pasarela y el servidor de dominio.

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración
Ancla (en modalidad ssh) - SSH	22	←	Servidor de dominio (en modalidad ssh)	
Ancla (en modalidad directa) - SSH		←	Servidor de dominio (en modalidad directa)	
Ancla (en modalidad ssh) - reenvío de túnel SSH	8497	↔	Servidor de dominio (en modalidad ssh)	
Ancla (en modalidad directa) - directa		←	Servidor de dominio (en modalidad directa)	
Pasarela - SSH	22	←	Servidor de dominio	

Comunicación local

Tabla 11. Configuración de comunicaciones de conectividad local de un servidor de dominio.

Comunicación local	Dirección	Propiedad de configuración
Servidor de dominio - registro de servicio local	↔	com.ibm.cdb.local.hostname
Servidor de dominio - servicios locales		
Servidor de dominio - 127.0.0.1		

Configuración de cortafuegos en un despliegue de servidor en modalidad continua

Es necesario configurar los cortafuegos en un despliegue de servidor de modalidad continua de manera que ciertos puertos específicos estén abierto para comunicación.

La figura siguiente muestra comunicación de TADDM en un despliegue de servidor de modalidad continua.

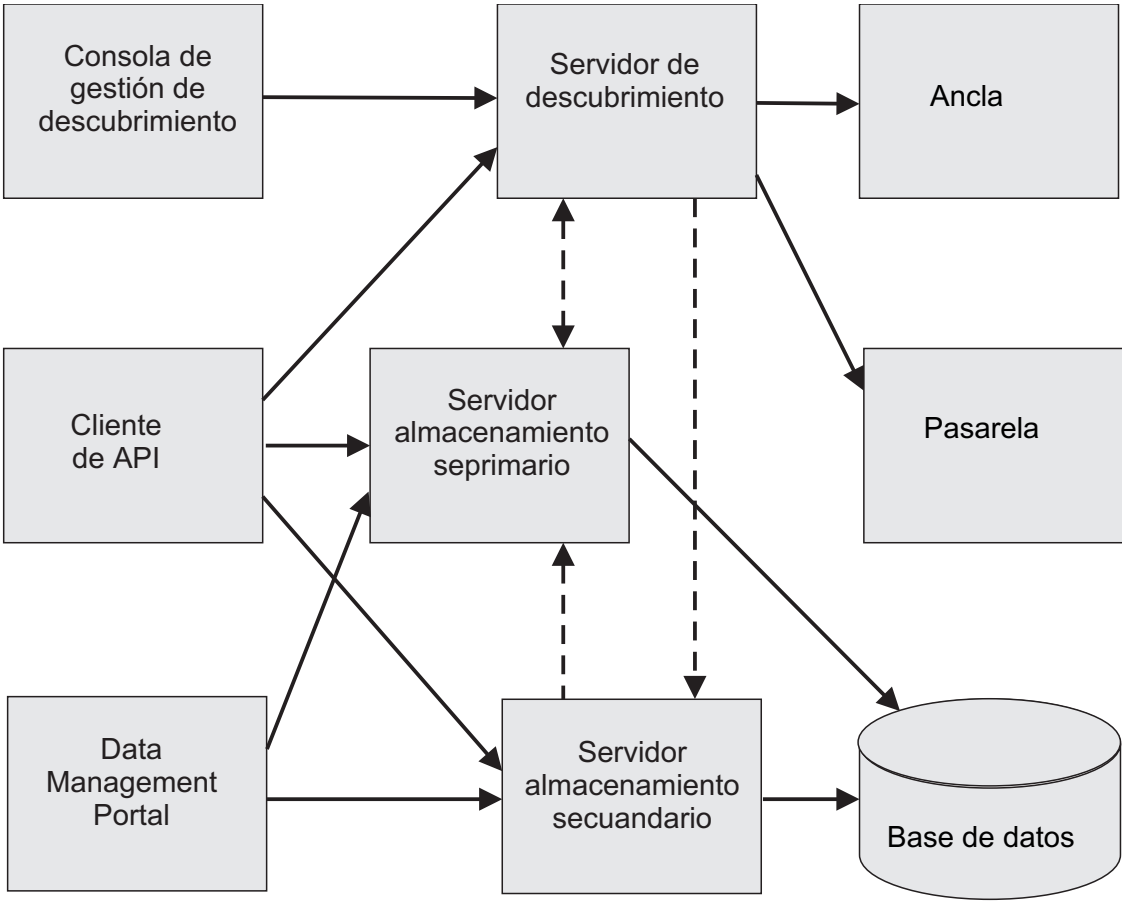

Figura 2. Comunicación de TADDM en un despliegue de servidor de modalidad continua

Servicios de conectividad:

Para el despliegue de un servidor en modalidad continua, puede configurar servicios de conectividad pública, entre servidores y local.

Importante: Los puertos predeterminados para las propiedades que se proporcionan más adelante en esta sección sólo se aplican a las propiedades que se listan en el archivo `collation.properties`. Si una propiedad no está codificada o está comentada en el archivo `collation.properties`, utiliza de forma predeterminada un puerto aleatorio. En especial, asegúrese de que la propiedad `com.ibm.cdb.service.RegistriesURLProvider.port` aparezca en el archivo `collation.properties`, para que el inicio sea satisfactorio.

Servicios de conectividad pública

La tabla siguiente muestra los valores de host predeterminados para los servicios de conectividad pública del servidor de almacenamiento primario, el servidor de almacenamiento secundario y el servidor de descubrimiento.

Tabla 12. Valores de host predeterminados para los servicios de conectividad pública del servidor de almacenamiento primario, el servidor de almacenamiento secundario y el servidor de descubrimiento

Nombre	Propiedad de configuración	Interfaz predeterminada
Host de servicio público	com.ibm.cdb.public.hostname	Definido por com.ibm.cdb.global.hostname

La tabla siguiente muestra los valores de puerto predeterminados para los servicios de conectividad pública del servidor de almacenamiento primario, el servidor de almacenamiento secundario y el servidor de descubrimiento.

Tabla 13. Valores de puerto predeterminados para los servicios de conectividad pública del servidor de almacenamiento primario, el servidor de almacenamiento secundario y el servidor de descubrimiento

Nombre	Propiedad de configuración	Protocolo	Puerto predeterminado
Puerto del servidor de la API	com.ibm.cdb.service.ApiServer.port	TCP	9530
Puerto de servidor de API seguro	com.ibm.cdb.service.SecureApiServer.secure.port	TCP	9531
Puerto HTTP (sin SSL)	com.ibm.cdb.service.web.port	TCP	9430
Puerto HTTPS (con SSL)	com.ibm.cdb.service.web.secure.port	TCP	9431
Puerto de comunicación del servidor de la GUI	com.ibm.cdb.service.ClientProxyServer.port	TCP	9435
Puerto de comunicación SSL del servidor de la GUI	com.ibm.cdb.service.SecureClientProxyServer.secure.port	TCP	9434
Puerto de registro de servicio público	com.ibm.cdb.service.registry.public.port	TCP	9433

Servicios de conectividad entre servidores

La tabla siguiente muestra los valores de host predeterminados para los servicios de conectividad entre servidores del servidor de almacenamiento primario y el servidor de almacenamiento secundario.

Tabla 14. Valores de host predeterminados para los servicios de conectividad entre servidores del servidor de almacenamiento primario y el servidor de almacenamiento secundario

Nombre	Propiedad de configuración	Interfaz predeterminada
Host de servicio entre servidores	com.ibm.cdb.interserver.hostname	Definido por com.ibm.cdb.global.hostname

La tabla siguiente muestra los valores de puerto predeterminados para los servicios de conectividad entre servidores del servidor de almacenamiento primario.

Tabla 15. Valores de puerto predeterminados para los servicios de conectividad entre servidores del servidor de almacenamiento primario

Nombre	Propiedad de configuración	Protocolo	Puerto predeterminado
Puerto de TopologyManager	com.ibm.cdb.service.TopologyManager.port	TCP	9550
Puerto de SecurityManager	com.ibm.cdb.service.SecurityManager.port	TCP	9540
Puerto de RegistriesURLProvider	com.ibm.cdb.service.RegistriesURLProvider.port	TCP	9560
Puerto de registro de servicio entre servidores	com.ibm.cdb.service.registry.interserver.port	TCP	4160

La tabla siguiente muestra los valores de puerto predeterminados para los servicios de conectividad entre servidores del servidor de almacenamiento secundario.

Tabla 16. Valores de puerto predeterminados para los servicios de conectividad entre servidores del servidor de almacenamiento secundario

Nombre	Propiedad de configuración	Protocolo	Puerto predeterminado
Puerto de TopologyManager	com.ibm.cdb.service.TopologyManager.port	TCP	9550
Puerto de RegistriesURLProvider	com.ibm.cdb.service.RegistriesURLProvider.port	TCP	9560
Puerto de registro de servicio entre servidores	com.ibm.cdb.service.registry.interserver.port	TCP	4160

Servicios de conectividad local

Los puertos de servicios locales no están definidos de forma explícita. Todos los puertos tienen que estar abiertos en la interfaz que esté definida para servicios locales. La interfaz predeterminada es el bucle de retorno.

La tabla siguiente muestra los valores de host predeterminados para los servicios de conectividad local del servidor de almacenamiento primario, el servidor de almacenamiento secundario y el servidor de descubrimiento.

Tabla 17. Valores de host predeterminados para los servicios de conectividad local del servidor de almacenamiento primario, el servidor de almacenamiento secundario y el servidor de descubrimiento

Nombre	Propiedad de configuración	Interfaz predeterminada
Host de servicio de área de conectividad local	com.ibm.cdb.local.hostname	127.0.0.1

Configuración de la comunicación en el despliegue del servidor en modalidad continua:

Para establecer correctamente la comunicación en el despliegue del servidor en modalidad continua, configure los servicios de conectividad pública, local y entre servidores.

En las siguientes tablas se muestran los elementos que puede conectar en el despliegue del servidor en modalidad continua y los puertos que debe abrir para que la comunicación se establezca correctamente.

Comunicación entre servidores

Tabla 18. Configuración de comunicaciones de conectividad entre servidores en el despliegue del servidor en modalidad continua.

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración	Soporte de TLS
Servidor de descubrimiento			**Servidor de almacenamiento primario**		
	9433	→	Servidor de almacenamiento primario	com.ibm.cdb. service.registry. public.port	Sí
	4160	→	Servidor de almacenamiento primario - Registro de servicio entre servidores	com.ibm.cdb. service.registry. interserver.port	No
	9560	→	Servidor de almacenamiento primario - Registros URLProvider	com.ibm.cdb. service.Registries URLProvider.port	Sí
	9540	→	Servidor de almacenamiento primario - SecurityManager	com.ibm.cdb. service.Security Manager.port	Sí
	9550	→	Servidor de almacenamiento primario - TopologyManager	com.ibm.cdb. service.Topology Manager.port	Sí
	9430	←	Servidor de almacenamiento primario - Web	com.ibm.cdb. service.web.port	No
Servidor de descubrimiento			**Servidor de almacenamiento secundario**		
	4160	→	Servidor de almacenamiento secundario - Registro de servicio entre servidores	com.ibm.cdb. service.registry. interserver.port	No
	9560	→	Servidor de almacenamiento secundario - Registros URLProvider	com.ibm.cdb. service.Registries URLProvider.port	Sí
	9550	→	Servidor de almacenamiento secundario - TopologyManager	com.ibm.cdb. service.Topology Manager.port	Sí

Tabla 18. Configuración de comunicaciones de conectividad entre servidores en el despliegue del servidor en modalidad continua. (continuación)

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración	Soporte de TLS
Servidor de almacenamiento secundario			**Servidor de almacenamiento primario**		
	4160	→	Servidor de almacenamiento primario - Registro de servicio entre servidores	com.ibm.cdb. service.registry. interserver.port	No
	9560	→	Servidor de almacenamiento primario - Registros URLProvider	com.ibm.cdb. service.Registries URLProvider.port	Sí
	9540	→	Servidor de almacenamiento primario - SecurityManager	com.ibm.cdb. service.Security Manager.port	Sí
	9550	→	Servidor de almacenamiento primario - TopologyManager	com.ibm.cdb. service.Topology Manager.port	Sí
Servidor de bases de datos	5000	←	**Servidor de almacenamiento primario**		No
Servidor de bases de datos	5000	←	**Servidor de almacenamiento secundario**		No

Comunicación entre el portal de gestión de descubrimiento; los clientes de API y los clientes del portal web y de Data Management Portal; y los servidores de TADDM

Tabla 19. Comunicación entre el portal de gestión de descubrimiento; los clientes de API y los clientes del portal web y de Data Management Portal; y los servidores de TADDM.

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración	Soporte de TLS
Portal de gestión de descubrimiento	9433	→	Servidor de descubrimiento - Registro de servicio público	com.ibm.cdb.service. registry.public.port	Sí
	9435	→	Servidor de descubrimiento - ClientProxyServer	com.ibm.cdb.service. ClientProxyServer.port	No
	9434	→	Servidor de descubrimiento - SecureClient ProxyServer	com.ibm.cdb.service. SecureClientProxy Server.secure.port	Sí

Tabla 19. Comunicación entre el portal de gestión de descubrimiento; los clientes de API y los clientes del portal web y de Data Management Portal; y los servidores de TADDM. (continuación)

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración	Soporte de TLS
Clientes de API	9433	→	• Servidor de descubrimiento - Registro de servicio público • Servidor de almacenamiento primario - Registro de servicio público • Servidor de almacenamiento secundario - Registro de servicio público	com.ibm.cdb.service.registry.public.port	Sí
	9530	→	• Servidor de descubrimiento - Servidor de API • Servidor de almacenamiento primario - Servidor de API • Servidor de almacenamiento secundario - Servidor de API	com.ibm.cdb.service.ApiServer.port	No
	9531	→	• Servidor de descubrimiento - Servidor de API seguro • Servidor de almacenamiento primario - Servidor de API seguro • Servidor de almacenamiento secundario - Servidor de API seguro	com.ibm.cdb.service.SecureApiServer.secure.port	Sí

Tabla 19. Comunicación entre el portal de gestión de descubrimiento; los clientes de API y los clientes del portal web y de Data Management Portal; y los servidores de TADDM. (continuación)

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración	Soporte de TLS
Clientes del portal web y de Data Management Portal	9430	→	• Servidor de descubrimiento - Web • Servidor de almacenamiento primario - Web • Servidor de almacenamiento secundario - Web	com.ibm.cdb.service.web.port	No
	9431	→	• Servidor de descubrimiento - Web segura • Servidor de almacenamiento primario - Web segura • Servidor de almacenamiento secundario - Web segura	com.ibm.cdb.service.web.secure.port	Sí

Comunicación entre el ancla y la pasarela y el servidor de descubrimiento

Tabla 20. Comunicación entre el ancla y la pasarela y el servidor de descubrimiento.

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración
Ancla (en modalidad ssh) - SSH	22	←	Servidor de descubrimiento (en modalidad ssh)	
Ancla (en modalidad directa) - SSH		←	Servidor de descubrimiento (en modalidad directa)	
Ancla (en modalidad ssh) - reenvío de túnel SSH	8497	↔	Servidor de descubrimiento (en modalidad ssh)	
Ancla (en modalidad directa) - directa		←	Servidor de descubrimiento (en modalidad directa)	
Pasarela - SSH	22	←	Servidor de descubrimiento	

Comunicación local

Tabla 21. Configuración de comunicaciones de conectividad local en el despliegue del servidor en modalidad continua.

Comunicación local	Dirección	Propiedad de configuración
Servidor de descubrimiento		

Tabla 21. Configuración de comunicaciones de conectividad local en el despliegue del servidor en modalidad continua. (continuación)

Comunicación local	Dirección	Propiedad de configuración
Servidor de descubrimiento - registro de servicio local	⟷	com.ibm.cdb.local.hostname
Servidor de descubrimiento - servicios locales		
Servidor de descubrimiento - 127.0.0.1		
Servidor de almacenamiento primario		
Servidor de almacenamiento primario - registro de servicio local	⟷	com.ibm.cdb.local.hostname
Servidor de almacenamiento primario - servicios locales		
Servidor de almacenamiento primario - 127.0.0.1		
Servidor de almacenamiento secundario		
Servidor de almacenamiento secundario - registro de servicio local	⟷	com.ibm.cdb.local.hostname
Servidor de almacenamiento secundario - servicios locales		
Servidor de almacenamiento secundario - 127.0.0.1		

Configuración de cortafuegos en un despliegue de servidor de sincronización

Es necesario configurar los cortafuegos en un despliegue de servidor de sincronización de manera que algunos puertos específicos estén abierto para comunicación.

La figura siguiente muestra comunicación de TADDM en un despliegue de servidor de sincronización.

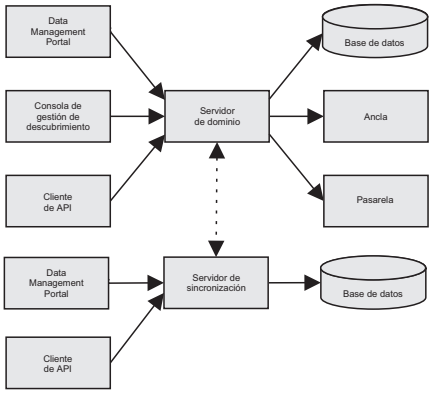

Figura 3. Comunicación de TADDM en un despliegue de servidor de sincronización

Configuración de los servicios de conectividad:

Para el despliegue de un servidor de sincronización, puede configurar servicios de conectividad pública, entre servidores y local.

Importante: Los puertos predeterminados para las propiedades que se proporcionan más adelante en esta sección sólo se aplican a las propiedades que se listan en el archivo `collation.properties`. Si una propiedad no está codificada o está comentada en el archivo `collation.properties`, utiliza de forma predeterminada un puerto aleatorio. En especial, asegúrese de que la propiedad `com.ibm.cdb.service.RegistriesURLProvider.port` aparezca en el archivo `collation.properties`, para que el inicio sea satisfactorio.

Servicios de conectividad pública

La tabla siguiente muestra los valores de host predeterminados para los servicios de conectividad pública del servidor de dominio y el servidor de sincronización.

Tabla 22. Valores de host predeterminados para los servicios de conectividad pública del servidor de dominio y el servidor de sincronización

Nombre	Propiedad de configuración	Interfaz predeterminada
Host de servicio público	com.ibm.cdb.public.hostname	Definido por com.ibm.cdb.global.hostname

La tabla siguiente muestra los valores de puerto predeterminados para los servicios de conectividad pública del servidor de dominio.

Tabla 23. Valores de host predeterminados para los servicios de conectividad pública del servidor de dominio

Nombre	Propiedad de configuración	Protocolo	Puerto predeterminado
Puerto del servidor de la API	com.ibm.cdb.service.ApiServer.port	TCP	9530
Puerto de servidor de API seguro	com.ibm.cdb.service.SecureApiServer.secure.port	TCP	9531
Puerto HTTP (sin SSL)	com.ibm.cdb.service.web.port	TCP	9430
Puerto HTTPS (con SSL)	com.ibm.cdb.service.web.secure.port	TCP	9431
Puerto de comunicación del servidor de la GUI	com.ibm.cdb.service.ClientProxyServer.port	TCP	9435
Puerto de comunicación SSL del servidor de la GUI	com.ibm.cdb.service.SecureClientProxyServer.secure.port	TCP	9434
Puerto de registro de servicio público	com.ibm.cdb.service.registry.public.port	TCP	9433

La tabla siguiente muestra los valores de puerto predeterminados para los servicios de conectividad pública del servidor de sincronización.

Tabla 24. Valores de puerto predeterminados para los servicios de conectividad pública del servidor de sincronización

Nombre	Propiedad de configuración	Protocolo	Puerto predeterminado
Puerto del servidor de la API	com.ibm.cdb.service.ApiServer.port	TCP	9530
Puerto de servidor de API seguro	com.ibm.cdb.service.SecureApiServer.secure.port	TCP	9531

Tabla 24. Valores de puerto predeterminados para los servicios de conectividad pública del servidor de sincronización (continuación)

Nombre	Propiedad de configuración	Protocolo	Puerto predeterminado
Puerto HTTP (sin SSL)	com.ibm.cdb.service.web.port	TCP	9430
Puerto HTTPS (con SSL)	com.ibm.cdb.service.web.secure.port	TCP	9431
Puerto de registro de servicio público	com.ibm.cdb.service.registry.public.port	TCP	9433

Servicios de conectividad entre servidores

La tabla siguiente muestra los valores de host predeterminados para los servicios de conectividad entre servidores del servidor de dominio y el servidor de sincronización.

Tabla 25. Valores de host predeterminados para los servicios de conectividad entre servidores del servidor de dominio y el servidor de sincronización

Nombre	Propiedad de configuración	Interfaz predeterminada
Host de servicio entre servidores	com.ibm.cdb.interserver.hostname	Definido por com.ibm.cdb.global.hostname

La tabla siguiente muestra los valores de puerto predeterminados para los servicios de conectividad entre servidores del servidor de dominio.

Tabla 26. Valores de puerto predeterminados para los servicios de conectividad entre servidores del servidor de dominio

Nombre	Propiedad de configuración	Protocolo	Puerto predeterminado
Puerto de TopologyManager	com.ibm.cdb.service.TopologyManager.port	TCP	9550
Puerto de SecurityManager	com.ibm.cdb.service.SecurityManager.port	TCP	9540
Puerto de RegistriesURLProvider	com.ibm.cdb.service.RegistriesURLProvider.port	TCP	9560
Puerto de registro de servicio entre servidores	com.ibm.cdb.service.registry.interserver.port	TCP	4160

La tabla siguiente muestra los valores de puerto predeterminados para los servicios de conectividad entre servidores del servidor de sincronización.

Tabla 27. Valores de puerto predeterminados para los servicios de conectividad entre servidores del servidor de sincronización

Nombre	Propiedad de configuración	Protocolo	Puerto predeterminado
Puerto de RegistriesURLProvider	com.ibm.cdb.service.RegistriesURLProvider.port	TCP	9560
Puerto de EnterpriseSecurityManager	com.ibm.cdb.service.EnterpriseSecurityManager.port	TCP	9570
Puerto de registro de servicio entre servidores	com.ibm.cdb.service.registry.interserver.port	TCP	4160

Servicios de conectividad local

Los puertos de servicios locales no están definidos de forma explícita. Todos los puertos tienen que estar abiertos en la interfaz que esté definida para servicios locales. La interfaz predeterminada es el bucle de retorno.

La tabla siguiente muestra los valores de host predeterminados para los servicios de conectividad local del servidor de dominio y el servidor de sincronización.

Tabla 28. Valores de host predeterminados para los servicios de conectividad local del servidor de dominio y el servidor de sincronización

Nombre	Propiedad de configuración	Interfaz predeterminada
Host de servicio local	com.ibm.cdb.local.hostname	127.0.0.1

Configuración de la comunicación en el despliegue de servidor de sincronización:

Para establecer correctamente la comunicación en el despliegue del servidor de sincronización, configure los servicios de conectividad pública, local y entre servidores.

En las siguientes tablas se muestran los elementos que puede conectar en el despliegue del servidor de sincronización y los puertos que debe abrir para que la comunicación se establezca correctamente.

Comunicación entre servidores

Tabla 29. Configuración de comunicaciones de conectividad entre servidores en el despliegue del servidor de sincronización.

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración
Servicio del dominio			**Servidor de sincronización**	
	4160	→	Servidor de sincronización - Registro de servicio entre servidores	com.ibm.cdb.service.registry.interserver.puerto
	9560	→	Servidor de sincronización - RegistriesURLProvider	com.ibm.cdb.service.RegistriesURL Provider.port
	9570	→	Servidor de sincronización - EnterpriseSecurityManager	com.ibm.cdb.service.EnterpriseSecurity Manager.port
Servicio del dominio			**Servidor de sincronización**	

Tabla 29. Configuración de comunicaciones de conectividad entre servidores en el despliegue del servidor de sincronización. (continuación)

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración
Servidor de dominio - Registro de servicio entre servidores	4160	←	Servidor de sincronización	com.ibm.cdb.service.registry.interserver.puerto
Servidor de dominio - Registros URLProvider	9560	←		com.ibm.cdb.service.RegistriesURL Provider.port
Servidor de dominio - Seguridad Gestor	9540	←		com.ibm.cdb.service.SecurityManager.port
Servidor de dominio - Topología Gestor	9550	←		com.ibm.cdb.service.TopologyManager.puerto
Servidor de bases de datos	5000	←	**Servicio del dominio**	
Servidor de bases de datos	5000	←	**Servidor de sincronización**	

Comunicación entre el portal de gestión de descubrimiento; los clientes de API y los clientes del portal web y de Data Management Portal; y los servidores de dominio y sincronización

Tabla 30. Comunicación entre el portal de gestión de descubrimiento; los clientes de API y los clientes de Data Management Portal; y los servidores de dominio y sincronización.

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración
Portal de gestión de descubrimiento	9433	→	Servidor de dominio - Registro de servicio público	com.ibm.cdb.service.registry.public.port
	9435	→	Servidor de dominio - ClientProxyServer	com.ibm.cdb.service.ClientProxyServer.puerto
	9434	→	Servidor de dominio - SecureClientProxyServer	com.ibm.cdb.service.SecureClientProxy Server.secure.port
Clientes de API	9433	→	• Servidor de dominio - Registro de servicio público • Servidor de sincronización - Registro de servicio público	com.ibm.cdb.service.registry.public.port
	9530	→	• Servidor de dominio - Servidor de API • Servidor de sincronización - Servidor de API	com.ibm.cdb.service.ApiServer.port
	9531	→	• Servidor de dominio - Servidor de API seguro • Servidor de sincronización - Servidor de API seguro	com.ibm.cdb.service.SecureApiServer.secure.port

Tabla 30. Comunicación entre el portal de gestión de descubrimiento; los clientes de API y los clientes de Data Management Portal; y los servidores de dominio y sincronización. (continuación)

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración
Clientes del portal web y de Data Management Portal	9430	→	• Servidor de dominio - Web • Servidor de sincronización - Web	com.ibm.cdb.service.web.port
	9431	→	• Servidor de dominio - Web segura • Servidor de sincronización - Web segura	com.ibm.cdb.service.web.secure.port

Comunicación entre el ancla y la pasarela y el servidor de dominio

Tabla 31. Comunicación entre el ancla y la pasarela y el servidor de dominio.

Elemento A	Puerto	Dirección	Elemento B	Propiedad de configuración
Ancla (en modalidad ssh) - SSH	22	←	Servidor de dominio (en modalidad ssh)	
Ancla (en modalidad directa) - SSH		←	Servidor de dominio (en modalidad directa)	
Ancla (en modalidad ssh) - reenvío de túnel SSH	8497	↔	Servidor de dominio (en modalidad ssh)	
Ancla (en modalidad directa) - directa		←	Servidor de dominio (en modalidad directa)	
Pasarela - SSH	22	←	Servidor de dominio	

Comunicación local

Tabla 32. Configuración de comunicaciones de conectividad local en el despliegue del servidor de sincronización.

Comunicación local	Dirección	Propiedad de configuración
Servicio del dominio		
Servidor de dominio - registro de servicio local	↔	com.ibm.cdb.local.hostname
Servidor de dominio - servicios locales		
Servidor de dominio - 127.0.0.1		
Servidor de sincronización		
Servidor de sincronización - registro de servicio local	↔	com.ibm.cdb.local.hostname
Servidor de sincronización - servicios locales		
Servidor de sincronización - 127.0.0.1		

Referencia de propiedades del servidor TADDM

El archivo `collation.properties` contiene propiedades para el servidor TADDM. Puede editar algunas de estas propiedades.

El archivo `collation.properties` se encuentra en el directorio `$COLLATION_HOME/etc`. El archivo contiene comentarios sobre cada una de las propiedades.

Si actualiza el archivo `collation.properties`, debe guardar el archivo y reiniciar el servidor para que el cambio surta efecto.

Propiedades con ámbito y sin ámbito

El archivo `collation.properties` contiene dos tipos de propiedades: con ámbito y sin ámbito.

propiedad con ámbito
Propiedad a la que puede añadir una dirección IP o el nombre de un conjunto de ámbitos. La dirección IP o el nombre del conjunto de ámbitos hacen que la propiedad dependa del host que se está descubriendo. Únicamente puede utilizar nombres de conjuntos de ámbitos que no contengan espacios, apóstrofos ('), puntos (.) y barras inclinadas (/).

propiedad sin ámbito
Propiedad que no puede restringir para que sea específica de un objeto.

Por ejemplo, las siguientes propiedades son propiedades sin ámbito:

- `com.collation.log.filesize`
- `com.collation.discover.agent.command.lsof.Linux`

Sin embargo, la propiedad `com.collation.discover.agent.command.lsof.Linux` puede ser una propiedad con ámbito si añade una dirección IP o un nombre de un conjunto de ámbitos, como se muestra en los siguientes ejemplos:

- Ejemplo de adición de dirección de IP `129.42.56.212`:
  ```
  com.collation.discover.agent.command.lsof.Linux.129.42.56.212=sudo lsof
  ```
- Ejemplo de adición de conjunto de ámbitos denominado “scope1”:
  ```
  com.collation.discover.agent.command.lsof.Linux.scope1=sudo lsof
  ```

Propiedades que no se deben modificar

Si se cambian ciertas propiedades del archivo `collation.properties` el sistema puede dejar de estar operativo.

Las siguientes propiedades no se deben modificar:

com.collation.version
Identifica la versión del producto.

com.collation.branch
Identifica la ramificación del código.

com.collation.buildnumber
Identifica el número de compilación. Este número se establece mediante el proceso de compilación.

com.collation.oalbuildnumber
Identifica el número de compilación de otro proceso de compilación.

com.collation.SshWeirdReauthErrorList=Permiso denegado
El valor de esta propiedad debe ser `Permission denied`.

La propiedad es necesaria porque los sistemas Windows niegan de manera aleatoria los intentos de inicio de sesión válidos. Puede intentarlo con el par de nombre de usuario y contraseña que haya funcionado anteriormente durante las ejecuciones de descubrimiento.

Propiedades del almacenamiento en memoria caché de las credenciales de acceso

Estas propiedades se aplican al almacenamiento en memoria caché de las credenciales.

com.ibm.cdb.security.auth.cache.disabled=false
El valor predeterminado es `false`.

Esta propiedad determina si está inhabilitado el almacenamiento en memoria caché de las credenciales.

Esta propiedad es una propiedad con ámbito y perfil. Puede añadir una dirección IP, el nombre de un conjunto de ámbitos o un nombre de perfil. También puede establecerla en la configuración del perfil en la consola de Discovery Management.

com.ibm.cdb.security.auth.cache.fallback.failed=true
El valor predeterminado es `true`.

Esta propiedad activa la reserva cuando una memoria caché contiene credenciales válidas pero, tras la recuperación, la validación falla. Si la reserva está habilitada y las credenciales almacenadas en memoria caché ya no son válidas, la memoria caché itera por todos los tipos de entradas de acceso disponibles hasta que encuentra una coincidencia.

Esta propiedad es una propiedad con ámbito y perfil. Puede añadir una dirección IP, el nombre de un conjunto de ámbitos o un nombre de perfil.

Las siguientes entradas son ejemplos de las entradas que puede encontrar en el archivo `collation.properties`:

```
com.ibm.cdb.security.auth.cache.fallback.failed=false
com.ibm.cdb.security.auth.cache.fallback.failed.10.160.160.11=true
com.ibm.cdb.security.auth.cache.fallback.failed.ScopeA=true
com.ibm.cdb.security.auth.cache.fallback.failed.GroupA=true
com.ibm.cdb.security.auth.cache.fallback.failed.Level_2_Discovery=false
```

También puede establecer esta propiedad en la consola de Discovery Management, desde el separador **Propiedades de plataforma** de la configuración del perfil.

com.ibm.cdb.security.auth.cache.fallback.invalid=true
El valor predeterminado es `true`.

Esta propiedad activa la reserva cuando una entrada que se ha leído en la memoria caché contiene un intento no válido (el último acceso ha fallado y no existen credenciales válidas). Si la reserva está habilitada, la memoria caché itera por todos los tipos de entradas de acceso disponibles hasta que encuentra una coincidencia.

Esta propiedad es una propiedad con ámbito y perfil, puede añadir una dirección IP, el nombre de un conjunto de ámbitos o un nombre de perfil.

Las siguientes entradas son ejemplos de las entradas que puede encontrar en el archivo `collation.properties`:

```
com.ibm.cdb.security.auth.cache.fallback.invalid=false
com.ibm.cdb.security.auth.cache.fallback.invalid.10.160.160.11=true
com.ibm.cdb.security.auth.cache.fallback.invalid.ScopeA=true
com.ibm.cdb.security.auth.cache.fallback.invalid.GroupA=true
com.ibm.cdb.security.auth.cache.fallback.invalid.Level_2_Discovery=false
```

También puede establecer esta propiedad en la consola de Discovery Management, desde el separador **Propiedades de plataforma** de la configuración del perfil.

Fix Pack 5 **com.ibm.cdb.security.auth.cache.itm.disabled=true**
El valor predeterminado es `true`.

Esta propiedad determina si está inhabilitado el almacenamiento en memoria caché de las credenciales para el descubrimiento de OSLC.

Esta propiedad es una propiedad con ámbito y perfil. Puede añadir una dirección IP, el nombre de un conjunto de ámbitos o un nombre de perfil. También puede establecerla en la configuración del perfil en la consola de Discovery Management.

Conceptos relacionados:

"Almacenamiento en memoria caché de las últimas credenciales correctas" en la página 14
TADDM puede almacenar en memoria caché las últimas credenciales de acceso que han funcionado. Se pueden volver a utilizar durante el siguiente descubrimiento (Nivel 2 o basado en script).

Propiedades del puerto de la interfaz de programación de aplicaciones (API)

Estas propiedades se aplican a los puertos de API.

com.ibm.cdb.service.ApiServer.port=9530
El valor predeterminado es `9530`. El valor debe ser un valor entero.

Esta propiedad especifica el puerto de escucha del servidor de API para solicitudes que no sean SSL. El valor se puede establecer en cualquier puerto disponible en el servidor. Cualquier cliente que utiliza la API para conectarse debe especificar este puerto para una conexión que no sea SSL.

com.ibm.cdb.service.SecureApiServer.secure.port=9531
El valor predeterminado es `9531`. El valor debe ser un valor entero.

Esta propiedad especifica el puerto de escucha del servidor de API para solicitudes que no sean SSL. El valor se puede establecer en cualquier puerto disponible en el servidor. Cualquier cliente que utiliza la API para conectarse debe especificar este puerto para una conexión SSL.

Propiedades de agentes de limpieza

Los agentes de limpieza eliminan los alias y los elementos de configuración huérfanos o arreglan las filas que faltan en las tablas. La mayoría lee las propiedades que se han definido en el archivo `collation.properties`.

AliasesCleanupAgent

El agente elimina los alias de la tabla ALIASES que ya no coinciden con los atributos de nombre del CI. También elimina los alias y las filas de la tabla PERSOBJ que no tengan ningún CI correspondiente. El agente lee las siguientes propiedades del archivo `collation.properties`:

Fix Pack 2 **com.ibm.cdb.topomgr.topobuilder.deleteAliasesWithoutMaster**
El valor predeterminado es `true`.

La propiedad especifica si los alias no tienen suprimido el alias maestro correspondiente en la tabla ALIASES. De forma predeterminada, la supresión está habilitada.

com.ibm.cdb.topomgr.topobuilder.max.row.fetch
El valor predeterminado es `1000`.

La propiedad configura el tamaño de lote para obtener alias de la tabla ALIASES.

Si establece la propiedad en `-1`, el agente no verifica los alias.

com.ibm.cdb.topomgr.topobuilder.max.row.delete
El valor predeterminado es `5000`.

La propiedad configura el tamaño de lote utilizado para suprimir alias.

Si establece la propiedad en `-1`, el agente no elimina los alias, sino que notifica únicamente aquellos que están corruptos.

com.ibm.cdb.topomgr.topobuilder.agents.AliasesCleanupAgent.maxNumber OfMastersToScan
El valor predeterminado es `1000`.

La propiedad configura el número de CI que requieren verificación de alias durante una única ejecución del agente.

com.ibm.cdb.topomgr.topobuilder.cleanupOrphanedAliasesAndPersobj
El valor predeterminado es `true`. El agente ejecuta la limpieza.

La propiedad habilita la limpieza de aquellos alias de la tabla ALIASES y los GUID de la tabla PERSOBJ que no tienen ningún CI correspondiente.

com.ibm.cdb.topomgr.topobuilder.DelayToRemoveAliases
El valor predeterminado es 12 (horas). El agente elimina los alias huérfanos con una antigüedad de más de 12 horas.

La propiedad define el tiempo en horas después de las cuales el agente suprime los alias sin un CI correspondiente. Protege los nuevos alias que podrían no tener un CI correspondiente porque no se ha completado el almacenamiento de CI.

Utilice esta propiedad con cuidado. No la establezca en un valor más pequeño.

AliasesJnTableCleanupAgent

Este agente elimina las filas antiguas de la tabla ALIASES_JN. Esta tabla contiene el historial de cambias de la tabla ALIASES. Se utiliza para buscar fusiones excesivas de elementos de configuración en la base de datos. El agente lee las siguientes propiedades del archivo `collation.properties`:

Fix Pack 2

com.ibm.cdb.topomgr.topobuilder.agents.AliasesJnTableCleanupAgent.maxRow
El valor predeterminado es `5000`. Se recomienda no cambiar el valor predeterminado.

Esta propiedad especifica el número máximo de filas suprimidas a la vez por el agente.

com.ibm.cdb.topomgr.topobuilder.agents.AliasesJnTableCleanupAgent.removeOlderThanDays
El valor predeterminado es 30 (días).

Esta propiedad elimina filas más antiguas que la hora especificada. De forma predeterminada, elimina las filas con una antigüedad superior a 30 días.

Si establece esta propiedad en 0 o en un valor más bajo, el agente se inhabilita.

com.ibm.cdb.topomgr.topobuilder.agents.AliasesJnTableCleanupAgent.timeout
El valor predeterminado es 1800 (segundos).

Esta propiedad especifica el periodo de tiempo después del cual se excede el tiempo de espera del agente. Si el periodo de tiempo especificado no es suficiente para suprimir todas las filas antiguas, el agente intenta suprimirlas en la próxima ejecución.

DependencyCleanupAgent

El agente elimina los objetos Relationship latentes. El agente lee las siguientes propiedades del archivo collation.properties:

com.ibm.cdb.topomgr.topobuilder.agents.DependencyCleanupAgent.timeout
El valor predeterminado en segundos es 600. Después de este tiempo, el agente deja de eliminar los objetos, aunque todavía quede alguno.

com.ibm.cdb.topomgr.topobuilder.agents.DependencyCleanupAgent.removeOlderThanDays
El valor predeterminado en días es 90. Los objetos Relationship que son anteriores al valor especificado se tratan como objetos latentes.

ObjectsWithoutAliasesCleanupAgent

El agente elimina los CI que no tienen alias en la tabla ALIASES. El agente lee la siguiente propiedad del archivo collation.properties:

com.ibm.cdb.topomgr.topobuilder.agents.ObjectsWithoutAliasesCleanupAgent.maxToRemove
El valor predeterminado es 1000

La propiedad limita el número de CI que el agente puede eliminar en una sola ejecución. Si establece la propiedad en -1, el agente sale sin realizar ninguna limpieza y muestra el mensaje ObjectsWithoutAliasesCleanupAgent is disabled.

PersobjCleanupAgent

El agente arregla todas las filas que faltan en la tabla PERSOBJ. No utiliza ninguna de las configuraciones del archivo collation.properties. El agente muestra un resumen del número de filas que se han arreglado, como en el siguiente ejemplo:

```
2012-08-22 18:12:21,500 TopologyBuilder [TopologyBuilderEngineThread$Cleanup@4.0]
INFO agents.PersobjCleanupAgent - Fixed 10 rows in PERSOBJ table
```

StorageExtentCleanupAgent

El agente elimina los objetos StorageExtent latentes. El agente lee las siguientes propiedades del archivo collation.properties:

com.ibm.cdb.topomgr.topobuilder.agents.StorageExtentCleanupAgent.timeout
El valor predeterminado en segundos es 1800. Después de este tiempo, el agente deja de eliminar los objetos, aunque todavía quede alguno.

com.ibm.cdb.topomgr.topobuilder.agents.StorageExtentCleanupAgent.removeOlderThanDays
El valor predeterminado en días es 1. Los objetos StorageExtent que son más de 1 día anteriores a su ComputerSystems padre se tratan como objetos latentes.

VlanInterfaceCleanupAgent

El agente elimina los objetos VlanInterface latentes. El agente lee las siguientes propiedades del archivo `collation.properties`:

com.ibm.cdb.topomgr.topobuilder.agents.VlanInterfaceCleanupAgent.timeout
El valor predeterminado en segundos es 1800. Después de este tiempo, el agente deja de eliminar los objetos, aunque todavía quede alguno.

com.ibm.cdb.topomgr.topobuilder.agents.VlanInterfaceCleanupAgent.removeOlderThanDays
El valor predeterminado en días es 1. Los objetos VlanInterface que son más de 1 día anteriores a su Vlans padre se tratan como objetos latentes.

Mandatos que pueden necesitar un privilegio superior

Estas propiedades especifican los mandatos del sistema operativo que TADDM utiliza y que pueden necesitar un privilegio superior, como autoridad root (o superusuario), para que se puedan ejecutar en el sistema de destino.

En general, sudo se utiliza en sistemas UNIX y Linux para proporcionar escalamiento de privilegio En vez de sudo, se pueden utilizar las alternativas siguientes:

- Habilite el derecho de acceso de setuid en el programa ejecutable de destino.
- Añada la cuenta de servicio de descubrimiento al grupo asociado con el programa ejecutable de destino.
- Utilice root como cuenta de servicio de descubrimiento (no es la preferente).

Para cada propiedad, sudo se puede configurar globalmente, lo que significa ejecutar el mandato con sudo en cada destino del sistema operativo o limitado a una dirección IP o a un conjunto de ámbitos específico.

Importante: En cada sistema de destino para el que se necesita escalamiento de privilegios, debe configurarse sudo con la opción NOPASSWD. De lo contrario, el descubrimiento se cuelga hasta que sudo excede el tiempo de espera.

com.collation.discover.agent.command.hastatus.Linux=sudo /opt/VRTSvcs/bin/hastatus
com.collation.discover.agent.command.haclus.Linux=sudo /opt/VRTSvcs/bin/haclus
com.collation.discover.agent.command.hasys.Linux=sudo /opt/VRTSvcs/bin/hasys
com.collation.discover.agent.command.hares.Linux=sudo /opt/VRTSvcs/bin/hares
com.collation.discover.agent.command.hagrp.Linux=sudo /opt/VRTSvcs/bin/hagrp
com.collation.discover.agent.command.hatype.Linux=sudo /opt/VRTSvcs/bin/hatype
com.collation.discover.agent.command.hauser.Linux=sudo /opt/VRTSvcs/bin/hauser

- Estas propiedades son necesarias para descubrir los componentes del Clúster Veritas.
- Para ejecutar estos mandatos sin sudo, la cuenta de servicio TADDM debe ser miembro del grupo de administración Veritas en el destino.

com.collation.discover.agent.command.vxdisk=vxdisk
com.collation.discover.agent.command.vxdg=vxdg
com.collation.discover.agent.command.vxprint=vxprint
com.collation.discover.agent.command.vxlicrep=vxlicrep
com.collation.discover.agent.command.vxupgrade=vxupgrade

- Estas propiedades descubren información de almacenamiento estándar de Veritas, además de información específica adicional de Veritas como grupo de discos, volúmenes, plexes y subdiscos de Veritas.

com.collation.platform.os.command.ps.SunOS=/usr/ucb/ps axww
com.collation.platform.os.command.psEnv.SunOS=/usr/ucb/ps axwweee
com.collation.platform.os.command.psParent.SunOS=ps -elf -o ruser,pid,ppid,comm
com.collation.platform.os.command.psUsers.SunOS=/usr/ucb/ps auxw

- Estas propiedades son necesarias para descubrir información de procesos en sistemas Solaris.

  Puede especificar una versión de Solaris determinada añadiendo el número de versión SunOS al nombre de la propiedad. Por ejemplo, la propiedad siguientes es específica de Solaris 10:

  ```
  com.collation.platform.os.command.ps.SunOS5.10=sudo /usr/ucb/ps axww
  ```

com.collation.platform.os.command.ps.Linux=ps axww
com.collation.platform.os.command.psEnv.Linux=ps axwweee
com.collation.platform.os.command.psParent.Linux=ps -ax -o ruser,pid,ppid,comm
com.collation.platform.os.command.psUsers.Linux=ps auxw

- Estas propiedades son necesarias para descubrir información de procesos en sistemas Linux.

com.collation.platform.os.command.ps.AIX=ps axww
com.collation.platform.os.command.psEnv.AIX=ps axwweee
com.collation.platform.os.command.psParent.AIX=ps -elf -o ruser,pid,ppid,comm
com.collation.platform.os.command.psUsers.AIX=ps auxw

- Estas propiedades son necesarias para descubrir información de procesos en sistemas AIX.

com.collation.platform.os.command.ps.HP-UX=sh UNIX95= ps -elfx -o pid,tty,state,time,args
com.collation.platform.os.command.psEnv.HP-UX=ps -eflx
com.collation.platform.os.command.psParent.HP-UX=sh UNIX95= ps -elfx -o ruser,pid,ppid,comm
com.collation.platform.os.command.psUsers.HP-UX=ps -efx

- Estas propiedades son necesarias para descubrir información de procesos en sistemas HP-UX.

com.collation.discover.agent.command.lsof.Vmnix=lsof
com.collation.discover.agent.command.lsof.Linux=lsof
com.collation.discover.agent.command.lsof.SunOS.1.2.3.4=sudo lsof
com.collation.discover.agent.command.lsof.Linux.1.2.3.4=sudo lsof
com.collation.discover.agent.command.lsof.HP-UX=lsof
com.collation.discover.agent.command.lsof.AIX=lsof

- Estas propiedades son necesarias para descubrir información de procesos o puertos.

  Puede especificar una versión de Solaris determinada añadiendo el número de versión SunOS al nombre de la propiedad. Por ejemplo, la propiedad siguientes es específica de Solaris 10:

  ```
  com.collation.discover.agent.command.lsof.SunOS5.10=sudo /usr/local/bin/lsof
  ```

com.collation.discover.agent.command.dmidecode.Linux=dmidecode
com.collation.discover.agent.command.dmidecode.Linux.1.2.3.4=sudo dmidecode

- Estas propiedades son necesarias para descubrir el fabricante, el modelo y el número de serie en sistemas Linux.

com.collation.discover.agent.command.vmcp.Linux=
Esta propiedad se puede utilizar para descubrir un ID de usuario invitado en un sistema virtual Linux de destino en ejecución en un sistema operativo z/VM.

com.collation.discover.agent.command.cat.SunOS=cat
com.collation.discover.agent.command.cat.SunOS.1.2.3.4=sudo cat

- Esta propiedad se utiliza para descubrir información de configuración para un cortafuegos de punto de comprobación en sistemas Solaris.

com.collation.discover.agent.command.interfacesettings.SunOS=sudo ndd
com.collation.discover.agent.command.interfacesettings.Linux=sudo mii-tool
com.collation.discover.agent.command.interfacesettings.SunOS.1.2.3.4=sudo ndd
com.collation.discover.agent.command.interfacesettings.Linux.1.2.3.5=sudo mii-tool
com.collation.discover.agent.command.interfacesettings.HP-UX=lanadmin
com.collation.discover.agent.command.interfacesettings.AIX=netstat

- Estas propiedades son necesarias para descubrir información de interfaz de red avanzada (velocidad de la interfaz, por ejemplo).

com.collation.discover.agent.command.adb.HP-UX=adb
com.collation.discover.agent.command.adb.HP-UX.1.2.3.4=sudo adb

- Esta propiedad es necesaria para descubrir información del procesador en sistemas HP.

com.collation.discover.agent.command.kmadmin.HP-UX=kmadmin
com.collation.discover.agent.command.kmadmin.HP-UX.1.2.3.4=sudo /usr/sbin/kmadmin

- Esta propiedad es necesaria para descubrir módulos de kernel en sistemas HP.

com.collation.platform.os.command.partitionTableListing.SunOS=prtvtoc

- Esta propiedad se utiliza para descubrir información de la tabla de particiones en sistemas Solaris.

com.collation.platform.os.command.lvm.lvdisplay.1.2.3.4=sudo lvdisplay -c
com.collation.platform.os.command.lvm.vgdisplay.1.2.3.4=sudo vgdisplay -c
com.collation.platform.os.command.lvm.pvdisplay.1.2.3.4=sudo pvdisplay -c

- Estas propiedades son necesarias para descubrir la información de volumen de almacenamiento.

com.collation.platform.os.command.lputil.SunOS.1.2.3.4=sudo /usr/sbin/lpfc/lputil

- Esta propiedad es necesaria para descubrir información HBA de canal de fibra Emulex en sistemas Solaris.

com.collation.platform.os.command.crontabEntriesCommand.SunOS=crontab -l
com.collation.platform.os.command.crontabEntriesCommand.Linux=crontab -l -u
com.collation.platform.os.command.crontabEntriesCommand.AIX=crontab -l
com.collation.platform.os.command.crontabEntriesCommand.HP-UX=crontab -l

- Estas propiedades son necesarias para descubrir las entradas **crontab**. Puede especificar estas propiedades como una propiedad con ámbito añadiendo una dirección IP o un nombre de conjunto de ámbitos a la propiedad. El ejemplo siguiente utiliza una dirección IP añadida:

  ```
  com.collation.platform.os.command.crontabEntriesCommand.AIX.1.2.3.4=crontab
  -l
  ```

com.collation.platform.os.command.filesystems.Linux=df -kTP
com.collation.platform.os.command.filesystems.SunOS=df -k | grep -v 'No such file or directory' | grep -v 'Input/output error' | awk '{print $1, $2, $4, $6}'
com.collation.platform.os.command.filesystems.AIX=df -k | grep -v 'No such file or directory' | grep -v 'Input/output error' | awk '{print $1, $2, $3, $7}
com.collation.platform.os.command.filesystems.HP-UX=df -kP | grep -v 'No such file or directory' | grep -v 'Input/output error' | grep -v Filesystem

- Estas propiedades son necesarias para descubrir sistemas de archivos.

com.collation.platform.os.command.fileinfo.ls=sudo ls
com.collation.platform.os.command.fileinfo.ls.1.2.3.4=sudo ls
com.collation.platform.os.command.fileinfo.cksum=sudo cksum
com.collation.platform.os.command.fileinfo.cksum.1.2.3.4=sudo cksum
com.collation.platform.os.command.fileinfo.dd=sudo dd
com.collation.platform.os.command.fileinfo.dd.1.2.3.4=sudo dd

- Estas propiedades son necesarias para la captura de archivos privilegiados.
- La captura de archivos privilegiados se utiliza en situaciones en las que la cuenta de servicio de descubrimiento no tiene acceso de lectura a los archivos de configuración de aplicaciones que son necesarios para el descubrimiento.

com.collation.discover.agent.WebSphereVersionAgent.versionscript=sudo
Esta propiedad se puede habilitar para acceder al archivo WebSphere `versionInfo.sh` si el usuario del descubrimiento no tiene acceso al sistema WebSphere Application Server de destino.

com.collation.platform.os.command.fileinfo.OnlyDirectoryRecursive
El indicador cambia la forma en que se descubren los archivos de configuración. El valor predeterminado es `False`.

Si cambia el indicador a `True`, el mecanismo no utiliza el mandato de búsqueda para descubrir reiteradamente el contenido de un directorio.

Cuando establece el indicador en `False`, este mecanismo utiliza el mandato de búsqueda para descubrir un archivo de forma reiterada, sin la ubicación exacta del archivo que se especifica.

Propiedades del servicio de menú contextual y del servicio de integración de datos

Estas propiedades se aplican al servicio del menú contextual (CMS) y al servicio de integración de datos (DIS).

com.ibm.cdb.DisCmsIntegration.enabled=true
El valor predeterminado es `true`.

Esta propiedad especifica si habilitar el agente compilador de topologías CMSDISAgent para que actualice periódicamente los datos de TADDM registrados con la base de datos del servicio de menú contextual y el servicio de integración de datos.

com.ibm.cdb.DisCmsIntegration.dbUser=*usuario*
Esta propiedad especifica el ID del usuario de la base de datos para la base de datos del servicio del menú contextual y el servicio de integración de datos.

com.ibm.cdb.DisCmsIntegration.dbPassword=*contraseña*
Esta propiedad especifica la contraseña del usuario de la base de datos del servicio del menú contextual y el servicio de integración de datos.

com.ibm.cdb.DisCmsIntegration.dbUrl=*url*
Esta propiedad especifica la URL de la base de datos para la base de datos del servicio del menú contextual y el servicio de integración de datos.

com.ibm.cdb.DisCmsIntegration.dbDriver=*controlador*
Esta propiedad especifica el controlador de la base de datos del servicio del menú contextual y el servicio de integración de datos.

com.ibm.cdb.DisCmsIntegration.changehistory.days_previous=30
El valor predeterminado es `30`.

Esta propiedad especifica el número de días de historial de cambio que se mostrará en los informes de cambios del servicio de menú contextual y del servicio de integración de datos.

Propiedades de la base de datos

Estas propiedades se aplican a la base de datos TADDM.

com.collation.db.password=contraseña
Esta propiedad especifica la contraseña de la base de datos, que se almacena en el servidor de TADDM, para el usuario de ésta.

com.collation.db.archive.password=contraseña
Esta propiedad especifica la contraseña de la base de datos, que se almacena en el servidor de TADDM, para el usuario de archivado de ésta.

com.ibm.cdb.db.max.retries
Esta propiedad especifica el número de reintentos para establecer la conexión con la base de datos.

com.ibm.cdb.db.timeout
Esta propiedad especifica el tiempo de hibernación (en milisegundos) entre los reintentos.

com.ibm.cdb.db.connection.ssl.enable=false
Esta propiedad especifica si la conexión con la base de datos se establece en la modalidad SSL para el usuario de base de datos.

El valor predeterminado es `false`.

com.ibm.cdb.db.connection.ssl.truststore.file=nombre_archivo
Esta propiedad especifica un archivo de almacén de confianza que se utiliza para establecer la conexión SSL con la base de datos para el usuario de base de datos. El archivo de almacén de confianza debe estar en el directorio `$COLLATION_HOME/etc/`.

com.ibm.cdb.db.connection.ssl.truststore.password=contraseña
Esta propiedad especifica una contraseña de almacén de confianza que se utiliza para establecer la conexión SSL con la base de datos para el usuario de base de datos.

com.ibm.cdb.db.archive.connection.ssl.enable=false
Esta propiedad especifica si la conexión con la base de datos se establece en la modalidad SSL para el usuario de base de datos de archivado.

El valor predeterminado es `false`.

com.ibm.cdb.db.archive.connection.ssl.truststore.file=nombre_archivo
Esta propiedad especifica un archivo de almacén de confianza que se utiliza para establecer la conexión SSL con la base de datos para el usuario de base de datos de archivado. El archivo de almacén de confianza debe estar en el directorio `$COLLATION_HOME/etc/`.

com.ibm.cdb.db.archive.connection.ssl.truststore.password=contraseña
Esta propiedad especifica una contraseña de almacén de confianza que se utiliza para establecer la conexión SSL con la base de datos para el usuario de base de datos de archivado.

Para cifrar las contraseñas de la base de datos en el archivo `collation.properties`, efectúe los siguientes pasos:

1. Edite el usuario de la base de datos o archive la contraseña de usuario mediante texto simple, o bien realice ambas opciones.
2. Detenga el servidor de TADDM.
3. Ejecute el archivo `encryptprops.sh` o el archivo `encryptprops.bat` (ubicado en el directorio `$COLLATION_HOME/bin`). Este script cifra las contraseñas.
4. Reinicie el servidor de TADDM.

Propiedades de descubrimiento

Estas propiedades se aplican al descubrimiento en general. Las propiedades del servidor TADDM que afectan a un sensor específico se documentan en la *Referencia de sensores* TADDM para cada sensor.

Fix Pack 4 **com.discover.anchor.maxChannelNumber**
Esta propiedad especifica la cantidad máxima de canales abiertos simultáneamente en la sesión de SSH entre el servidor TADDM y el ancla. Si la cantidad de canales abiertos es demasiado alta, el descubrimiento puede permanecer en dicho ancla y se puede agotar el tiempo de espera de los sensores incluidos en dicho ámbito. En dichos casos, utilice esta propiedad para controlar la cantidad de canales abiertos.

El valor predeterminado es `50`.

Fix Pack 4 **com.collation.platform.os.copyToLocal.preferScpCommand**
Esta propiedad especifica si el mandato externo **scp** se utiliza para copiar archivos de hosts remotos, normalmente objetivos de descubrimiento, al servidor TADDM. El mandato externo **scp** se define en la propiedad `com.collation.platform.os.scp.command`. Para habilitar el uso de un mandato externo **scp**, establece la propiedad en `true`.

El valor predeterminado de esta propiedad es `false`.

Nota: La propiedad se aplica solo a las sesiones SSH que se establecen con un inicio de sesión basado en claves (consulte "Configuración del descubrimiento mediante Secure Shell (SSH)" en la página 119). En caso de una autenticación con un nombre de usuario y una contraseña, el mandato

interno **scp** se utiliza independientemente del valor de la propiedad com.collation.platform.os.copyToLocal.preferScpCommand.

Esta propiedad es una propiedad con ámbito. Pueden añadir una dirección IP o el nombre de un ámbito definido para la propiedad. Por ejemplo:

```
com.collation.platform.os.copyToLocal.preferScpCommand.12.234.255.4=true
```

com.collation.platform.os.scp.command

Esta propiedad especifica la ruta al mandato **scp** del sistema operativo. Se puede utilizar cuando un cliente SSH no puede enviar archivos entre el servidor TADDM y los hosts remotos, normalmente, objetivos de descubrimiento. También puede utilizar un mandato alternativo pero debe tener la misma sintaxis que el mandato **scp**.

El valor de ejemplo: /usr/local/bin/scp.

Fix Pack 3 **com.collation.platform.session.ssh.winAuth**

Esta propiedad especifica si se intenta el inicio de sesión con las credenciales de Windows cuando se utiliza la sesión SSH. El valor predeterminado es true.

Puede establecer el valor en false, si no hay riesgo de que durante el descubrimiento haya intentos de iniciar sesión en servidores no Windows con las credenciales de Windows. Puede impedir el bloqueo de las cuentas de Windows Active Directory.

Fix Pack 3 **com.collation.platform.os.ignoreL2InterfaceDescription**

Esta propiedad especifica las descripciones de las L2Interfaces descubiertas que desee que se omitan durante el cálculo de la firma del sistema. Por ejemplo, si no desea que se utilice Microsoft Load Balancer Interface para calcular la firma de un sistema, especifique el valor siguiente:

```
com.collation.platform.os.ignoreL2InterfaceDescription=Microsoft Load
Balancer Interface
```

El valor de esta propiedad se tratará como una expresión regular. Esto significa que puede añadir más de una descripción de interfaz, y que no necesita utilizar ningún separador, como por ejemplo una coma.

Fix Pack 3 **com.ibm.cdb.topomgr.topobuilder.agents.Connection DependencyAgent2.dependencyPlaceholders**

Si esta propiedad se establece en true, crea servidores de aplicaciones de contenedor para las dependencias no descubiertas.

Nota: Esta propiedad no está incluida en el archivo collation.properties de forma predeterminada. Debe añadirla allí.

Cuando establezca el valor en true por primera vez, debe reiniciar TADDM para habilitar los atributos ampliados para las clases LogicalConnection y SSoftwareServer. Estos atributos ampliados son necesarios para el correcto funcionamiento de esta característica.

Para obtener más información sobre los marcadores de posición, consulte “Configuración del descubrimiento de marcadores de posición” en la página 134.

com.collation.platform.session.EncodingOverRide

Esta propiedad especifica el tipo de codificación que se utiliza durante una sesión de descubrimiento. Es especialmente útil cuando los servidores de destino utilizan una codificación diferente que la del servidor TADDM.

El valor de esta propiedad es el nombre de la codificación, por ejemplo `UTF-8`. No está incluido en el archivo `collation.properties` de forma predeterminada, debe añadirlo aquí.

También puede añadir un ámbito o una dirección IP a la propiedad. Por ejemplo:

```
com.collation.platform.session.EncodingOverRide.37.53.105.24=UTF-8
```

com.collation.discover.anchor.forceDeployment=true

El valor predeterminado es `true`.

Esta propiedad especifica si las anclas para el ámbito descubierto se despliegan durante el inicio.

Si define el valor en `false`, las anclas se despliegan sólo si se cumplen las siguientes condiciones:

- Si alguna dirección de IP del ámbito no puede recibir ping
- Si el puerto 22 no se puede alcanzar en ninguna de las direcciones de IP descubiertas.

Si existen anclas encadenadas, esta condición, se aplica a todas las anclas de la cadena. Si ancla de la cadena está restringida por una condición, las anclas anteriores deben cumplir dicha la condición para que todas las anclas puedan desplegarse.

com.collation.discover.anchor.lazyDeployment=false

El valor predeterminado es `false`.

Esta propiedad especifica si los archivos que requiere el sensor se copian cuando se despliega un ancla (un valor `false`) o cuando el sensor que requieren los archivos está a punto de iniciarse (un valor de `true`).

Por ejemplo, el sensor de IBM WebSphere tiene dependencias en el directorio `dist/lib/websphere`. El tamaño del directorio es de 130 MB. Si el valor de la propiedad es `false`, los datos de dependencia se copian en el host de destino cuando se despliega el ancla. Si el valor es `true`, los datos se copian cuando el sensor de WebSphere está a punto de ejecutarse en el ancla. Si no se ejecuta ningún sensor de WebSphere a través del ancla, se envían 130 MB al host remoto.

com.collation.discover.DefaultAgentTimeout=600000

Este valor es `600000` (en milisegundos), que es 10 minutos.

Esta propiedad especifica el tiempo de espera para los sensores en milisegundos. El tiempo de espera predeterminado no debe modificarse. En su lugar, se puede especificar el tiempo de espera para sensores individuales.

Para alterar temporalmente el tiempo de espera para un sensor particular, añada la línea siguiente en el archivo `collation.properties`:

```
com.collation.discover.agent.nombre_sensorSensor.timeout=
  tiempo_en_milisegundos
```

Por ejemplo:

```
com.collation.discover.agent.OracleSensor.timeout=1800000
```

com.collation.IpNetworkAssignmentAgent.defaultNetmask=*lanzar_ip-finalizar_ip/máscara de red*[, ...]

Esta propiedad define cómo las direcciones IP descubiertas durante un descubrimiento de nivel 1 se asignan a las subredes generadas. Un descubrimiento de nivel 1 no descubre subredes. En su lugar, se generan

objetos IpNetwork para contener cualquier interfaz que no esté asociada a una subred existente descubierta durante un descubrimiento de nivel 2 o nivel 3. Esta propiedad de configuración define qué objetos IpNetwork se deben crear, y cuántos nodos debe contener cada subred. (También se aplica a cualquier interfaz descubierta durante un descubrimiento de nivel 2 o de nivel 3 que, por algún motivo, no se puede asignar a una subred descubierta.)

El valor de esta propiedad consta de una única línea que contiene una o más entradas separadas por comas. Cada entrada describe un rango de direcciones IP en formato decimal separado por puntos IPv4, junto con una máscara de subred que se ha especificado como un valor entero entre 8 y 31. Las interfaces descubiertas en el rango especificado se colocan en las subredes creadas que no sean mayores que el tamaño especificado por la máscara de subred.

Por ejemplo, el valor siguiente define dos rangos de direcciones de subred con máscaras de subred diferentes:

```
9.0.0.0-9.127.255.255/23, 9.128.0.0-9.255.255.255/24
```

Los rangos de direcciones especificados se pueden solapar. Si una dirección IP descubierta coincide con más de un rango definido, se asigna a la primera subred coincidente tal como aparecen listadas en el valor de la propiedad.

Tras haber creado o cambiado esta propiedad de configuración y haber reiniciado el servidor de TADDM, todos los descubrimientos de nivel 1 posteriores utilizarán las subredes descubiertas. Para volver a asignar los objetos IpInterface existentes en la base de datos TADDM, acceda al directorio `$COLLATION_HOME/bin` y ejecute uno de los mandatos siguientes:

- **`adjustL1Networks.sh`** (sistemas Linux y UNIX)
- **`adjustL1Networks.bat`** (sistemas Windows)

Si el valor no se especifica correctamente, se muestran los mensajes correspondientes sólo cuando se ejecuta el programa de utilidad de línea de mandatos **`adjustL1Networks.sh`** (sistemas Linux y UNIX) o **`adjustL1Networks.bat`** (sistemas Windows). En caso contrario, los mensajes se colocan en el archivo `TopologyBuilder.log` del directorio `$COLLATION_HOME/log/services` y en el archivo `IpNetworkAssignmentAgent.log` del directorio `$COLLATION_HOME/log/agents`.

Este script vuelve a asignar todos los objetos IpInterface descubiertos durante los descubrimientos de nivel 1 a las subredes apropiadas, tal como se describe en la propiedad de configuración. Todo objeto IpNetwork generado que no contenga ninguna interfaz se suprime de la base de datos. Una vez finalizado el script, es posible que la interfaz de TADDM muestre varias notificaciones de los componentes cambiados debido a los objetos modificados. Puede borrar estas notificaciones actualizando la ventana.

Nota: Para poder utilizar este mandato, asegúrese de que se esté ejecutando el servidor de TADDM y de que no haya en curso ningún descubrimiento ni ninguna operación de carga masiva. Este script no lo soporta el servidor de sincronización.

`com.collation.number.persist.discovery.run=30`
El valor predeterminado es `30`.

Especifica el número de descubrimientos para los que se guarda información en el historial de descubrimiento en el portal de gestión de datos y en la consola de Discovery Management.

Para cambiar el valor predeterminado de un despliegue de servidor de modalidad continua, escriba el valor nuevo en el servidor de almacenamiento primario.

com.collation.platform.os.hostappdescriptorfiles.dir="*vía_de_acceso***"**
Especifica la vía de acceso completa cualificada en el directorio en el que se despliegan los archivos del descriptor de la aplicación para los sistemas informáticos (hosts). Esta propiedad es necesaria si desea añadir sistemas informáticos a las aplicaciones empresariales mediante descriptores de la aplicación. Puede determinar el ámbito de esta propiedad a un nombre de host específico o una dirección IP para especificar un ubicación diferente para cada host. En los ejemplos siguientes se muestra cómo especificar la vía de acceso del descriptor de la aplicación de host:

- Sistemas Linux y UNIX: `/home/taddm/hostappdescriptors`
- Sistemas Windows: `c://taddm//hostappdescriptors`

com.collation.platform.session.GatewayForceSsh
Especifica si debe forzarse a la pasarela a actuar de forma independiente respecto al ancla. Los valores válidos son *true* y *false*. Establezca el valor como `true` para resolver los problemas de Cygwin cuando tanto la pasarela como el ancla están en el mismo sistema. Cuando el valor se establece como verdadero (true), se utiliza una sesión SSH para transferir el tráfico entre la pasarela y el ancla en lugar de una sesión local.

com.collation.rediscoveryEnabled=`false`
El valor predeterminado es `false`.

Esta propiedad se aplica al redescubrimiento de un elemento de configuración que ya se ha descubierto. La funcionalidad de redescubrimiento está disponible en el portal de gestión de datos.

Restricción: El redescubrimiento no puede utilizar las credenciales de un perfil personalizado, utiliza las credenciales de la lista global.

Nota:

Para habilitar el redescubrimiento en un despliegue de servidor de dominio, defina el valor como `true` en el servidor de dominio.

Para habilitar el redescubrimiento en un despliegue de servidor de modalidad continua, defina el valor como `true` en el servidor de descubrimiento y el servidor de almacenamiento.

Redescubrimiento en un despliegue de servidor de modalidad continua
Cuando se utiliza el redescubrimiento en un despliegue de servidor de modalidad continua, se puede descubrir un elemento de configuración mediante diferentes servidores de descubrimiento, pero únicamente el último servidor de descubrimiento que haya descubierto el elementos de configuración es el que puede redescubrir el elemento de configuración. Como hay varios servidores de descubrimiento, cada servidor de descubrimiento sobrescribe la información de redescubrimiento del elemento de configuración.

Cuando se habilita el redescubrimiento en un servidor de descubrimiento, para cada objeto descubierto, se crea información adicional sobre el redescubrimiento.

Cuando se habilita el redescubrimiento en un servidor de almacenamiento, cada objeto descubierto se almacena con información adicional sobre el redescubrimiento.

Si se habilita el redescubrimiento en el servidor de descubrimiento, pero se inhabilita en el servidor de almacenamiento, no estará disponible la información sobre el redescubrimiento en la base de datos de TADDM. Además, debe asegurarse de que se utilizan las mismas credenciales para el servidor de descubrimiento y el servidor de almacenamiento.

com.ibm.cdb.discover.sensor.sys.utilization.workingdir=/tmp/taddm
El valor predeterminado es `/tmp/taddm`.

Esta propiedad especifica la vía de acceso raíz de los scripts del sensor de IBM Tivoli Utilization que se han de ejecutar en el sistema de destino. Si este valor no se especifica, se utiliza la vía de acceso definida por la propiedad `com.ibm.cdb.taddm.script.path`.

com.ibm.cdb.locationTag
Especifica el atributo de etiqueta de ubicación para cada elemento de configuración (CI) creado en el servidor de TADDM. El atributo de etiqueta de ubicación, que identifica la ubicación de un CI, se utiliza para soportar las etiquetas de ubicación estáticas. Antes de especificar esta etiqueta, es necesario definir el valor `com.ibm.cdb.locationTaggingEnabled` como `true`.

com.ibm.cdb.locationTaggingEnabled=false
El valor predeterminado es `false`.

Especifica si la funcionalidad del etiquetado de ubicación se habilita. Defina el valor de esta propiedad como `true` para:

- Especificar un atributo de etiqueta de ubicación para cada elemento de configuración (CI) creado en el servidor de TADDM (etiquetas de ubicación estáticas). Consulte la propiedad `com.ibm.cdb.locationTag` para obtener más detalles.
- Especificar una etiqueta de ubicación dinámica para los elementos de configuración (CI) creados durante un descubrimiento único. Para ello, utilice la interfaz de línea de mandatos (CLI). Las etiquetas de ubicación dinámicas sustituyen a las etiquetas de ubicación que ya existen (etiquetas de ubicación estáticas).
- Especifique una etiqueta de ubicación dinámica para los elementos de configuración (CI) creados al cargar datos mediante el programa de carga masiva.
- Especifique un valor de etiqueta de ubicación al ejecutar un informe BIRT para filtrar únicamente los datos y la información de los informes acerca de la ubicación especificada.
- Cree un valor de etiqueta de ubicación para los elementos de configuración creados durante un proceso de generación de tipología.

com.ibm.cdb.taddm.host
Especifica el alias de host del servidor de TADDM. Si este valor no se especifica, se utiliza el nombre de host del sistema. Si el servidor de TADDM no puede resolver el nombre de host del sistema, o si resuelve el host local, deberá especificar esta propiedad de forma manual.

com.ibm.cdb.taddm.script.path=/tmp/taddm
El valor predeterminado es /tmp/taddm.

Esta propiedad especifica la vía de acceso raíz para los scripts del sensor que se han de ejecutar en el sistema de destino. En esta ubicación se crea un árbol de subdirectorios que utiliza el formato: alias_host/número_descubrimiento/nombre_sensor. El nombre alias_host se recupera de la propiedad com.ibm.cdb.taddm.host. Si esta propiedad no se especifica, se utiliza el nombre de host del sistema. Para diferenciar entre descubrimientos simultáneos en el mismo servidor de descubrimiento, se asigna un número al directorio número_descubrimiento. Los scripts de descubrimiento y los resultados del descubrimiento se almacenan con esta estructura de directorios.

com.collation.discover.agent.signature.ignore.*1.2.3.4*=true
Esta propiedad se utiliza para omitir una dirección IP durante el cálculo de firma.

En el caso de algunas configuraciones, la firma de un sistema puede que no sea exclusiva, lo que genera problemas durante la reconciliación con las entradas existentes en la base de datos de TADDM. Por ejemplo, puede ocurrir cuando utiliza máquinas virtuales con tarjetas de red virtuales que tienen una dirección de hardware y una dirección IP válidas. En estos casos, debe excluir el cálculo de firma y utilizar otras reglas de denominación, por ejemplo, Modelo de producto, Fabricante o Número de serie.

Para cada dirección IP que desea ignorar, añada la propiedad com.collation.discover.agent.signature.ignore.*1.2.3.4*=true, donde *1.2.3.4* es la dirección IP que se va a ignorar.

Si desea ignorar muchas direcciones IP, puede crear un ámbito de descubrimiento. Añada la propiedad com.collation.discover.agent.signature.ignore.*lista_negra*=true al archivo collation.properties, donde *lista_negra* es el ámbito de descubrimiento con todas las direcciones IP que se van a ignorar.

Propiedades de descubrimiento avanzadas:

Las propiedades avanzadas de descubrimiento especifican la capacidad de almacenamiento intermedio para el almacenamiento de elementos de trabajo, el número de reinicios de elementos de descubrimiento concretos o el valor de tiempo para la impresión de estadísticas en un registro. No cambie estas propiedades a menos que se deben ajustar el proceso de descubrimiento con gran precisión.

com.ibm.cdb.discover.buffers.workitem.capacity=64
El valor predeterminado es 64. Sin embargo, este valor siempre es el doble del valor de com.collation.discover.dwcount, que es 32 de forma predeterminada.

Esta propiedad especifica la capacidad del almacenamiento intermedio para almacenar elementos de trabajo de descubrimiento. Se utiliza para limitar los requisitos de memoria del proceso de descubrimiento y así evitar errores de OutOfMemory. Para cada descubrimiento, se inicia un nuevo sensor.

No defina el valor para que sea menor que el número de trabajadores de descubrimiento que se especifican en com.collation.discover.dwcount, porque de lo contrario algunos de ellos quedan en estado desocupado.

com.ibm.cdb.discover.buffers.workitem.maxresets=10
El valor predeterminado es 10.

Esta propiedad especifica el número de veces que un sensor puede reiniciarse en caso de una anomalía inesperada, como una anomalía de una máquina virtual Java de TADDM que sea responsable del descubrimiento.

Además, el número de reinicios de un elemento del proceso de descubrimiento está limitado por com.ibm.cdb.discover.runrestartlimit, que especifica el número de reinicios de descubrimiento.

com.ibm.cdb.discover.buffers.seed.capacity=100
El valor predeterminado es 100.

Esta propiedad especifica la capacidad del almacenamiento intermedio para almacenar elementos de trabajo de inicio. Se utiliza para limitar los requisitos de memoria del proceso de descubrimiento y así evitar errores de OutOfMemory.

com.ibm.cdb.discover.buffers.result.capacity=100
El valor predeterminado es 100.

Esta propiedad especifica la capacidad del almacenamiento intermedio para almacenar elementos de trabajo de resultado. Se utiliza para limitar los requisitos de memoria del proceso de descubrimiento y así evitar errores de OutOfMemory. Para cada elemento de trabajo de resultado, se puede iniciar un nuevo sensor.

Defina el valor al mismo tamaño que com.ibm.cdb.discover.buffers.discovered.capacity.

com.ibm.cdb.discover.buffers.result.maxresets=10
El valor predeterminado es 10.

Esta propiedad especifica el número de veces que un proceso de descubrimiento puede iniciar un nuevo sensor para un elemento de trabajo de resultado en caso de una anomalía inesperada, como una anomalía de una máquina virtual Java de TADDM que sea responsable del descubrimiento.

Además, el número de reinicios de un elemento del proceso de descubrimiento está limitado por com.ibm.cdb.discover.runrestartlimit, que especifica el número de reinicios de descubrimiento.

com.ibm.cdb.discover.buffers.discovered.capacity=100
El valor predeterminado es 100.

Esta propiedad especifica la capacidad del almacenamiento intermedio para almacenar elementos de trabajo descubiertos. Cada elemento de trabajo descubierto representa un resultado de descubrimiento que está almacenado en la base de datos.

No especifique que este valor sea menor que el número de trabajadores de hebras de grabación de la base de datos que se especifican en com.collation.discover.topopumpcount.

com.ibm.cdb.discover.buffers.statistics.interval.seconds=60
El valor predeterminado es 60. Especifique el valor en segundos.

Esta propiedad especifica el valor tiempo para guardar las estadísticas del almacenamiento intermedio de descubrimiento en un registro. El registro se encuentra en /log/services/DiscoveryState.log.

com.ibm.cdb.discover.buffers.timeout.interval.seconds=600
El valor predeterminado es 600, que es 10 minutos. Especifique el valor en segundos.

Esta propiedad especifica el valor de tiempo para la comprobación de los elementos de trabajo para el tiempo de espera excedido.

com.ibm.cdb.discover.runcontroller.statistics.interval.seconds=60
El valor predeterminado es 60. Especifique el valor en segundos.

Esta propiedad especifica el valor tiempo para guardar las estadísticas de ejecución de descubrimiento en un registro. El registro está en /log/services/DiscoveryRunController.log.

com.ibm.cdb.discover.runrestartlimit=11
El valor predeterminado es 11.

Esta propiedad especifica el número de veces que se un descubrimiento sin inicializar se puede reiniciar después de una anomalía. El descubrimiento está en el estado sin inicializar cuando el proceso aún no se ha iniciado para todos los elementos del ámbito del descubrimiento.

com.collation.discovery.oracle.tablelimit=1000
El valor predeterminado es 1000. La propiedad solo da soporte a valores positivos.

Esta propiedad controla la cantidad de tablas descubiertas por el sensor de Oracle.

Propiedades de descubrimiento simultáneas:

Estas propiedades se aplican al descubrimiento simultáneo.

com.collation.discover.concurrent.discovery=true
El valor predeterminado es true.

Esta propiedad se utiliza para habilitar el descubrimiento simultáneo.

com.collation.discover.max.concurrent.discoveries=10
El valor predeterminado es 10.

Esta propiedad define el número máximo de descubrimientos simultáneos.

Propiedades de descubrimiento asíncrono:

Estas propiedades se aplican al descubrimiento asíncrono.

com.ibm.cdb.discover.asd.AsyncDiscoveryResultsDirectory=var/asdd
El valor predeterminado es var/asdd, que es relativo al directorio com.collation.home.

Esta propiedad define la ubicación del directorio raíz para los archivos de archivado en el servidor de TADDM que contiene resultados de descubrimiento asíncronos. La ubicación puede ser una vía de acceso relativa o absoluta. Una vía de acceso relativa es relativa al directorio com.collation.home.

com.ibm.cdb.discover.asd.ProcessUnreachableIPs=false
El valor predeterminado es false.

Esta propiedad se utiliza para habilitar el procesamiento de direcciones IP inaccesibles, que se utilizan en el descubrimiento asíncrono. Para habilitar el procesamiento de estas direcciones, defina el valor en true.

com.ibm.cdb.tarpath=tar

El valor predeterminado es `tar`.

Esta propiedad define la vía de acceso del mandato **tar** *en el servidor TADDM* del descubrimiento asíncrono.

En los sistemas operativos, como AIX o Linux, esta propiedad normalmente no es necesaria debido a que el mandato **tar** ya está instalado y disponible. Sin embargo, para generar un paquete de script de descubrimiento asíncrono o para procesar los archivos de archivado del descubrimiento en un servidor de TADDM que se ejecute en un sistema operativo Windows, debe instalar un programa tar de terceros y especificar la vía de acceso completa de ese programa.

El ejemplo siguiente muestra cómo especificar la vía de acceso del mandato **tar** en el servidor TADDM para el sistema operativo AIX:

```
com.ibm.cdb.tarpath=tar
```

com.ibm.cdb.targettarpath=tar

El valor predeterminado es `tar`.

Esta propiedad define la vía de acceso del mandato **tar** en el sistema de destino en el descubrimiento asíncrono.

En los sistemas operativos de destino, como AIX o Linux, esta propiedad normalmente no es necesaria debido a que el mandato **tar** ya está instalado y disponible. Sin embargo, para generar archivos de archivado de descubrimiento en los sistemas operativos Solaris, debido a una limitación en la longitud de los nombres de archivos, debe utilizar el programa de utilidad de archivado gtar y debe especificar la vía de acceso del programa de utilidad.

Los ejemplos siguientes muestran cómo especificar la vía de acceso del mandato **tar** *en el sistema de destino*, en función del sistema operativo:

Para AIX

```
com.ibm.cdb.targettarpath.AIX=tar
```

Para Solaris

```
com.ibm.cdb.targettarpath.SunOS=/usr/sfw/bin/gtar
```

Propiedades de descubrimiento basado en script:

Estas propiedades se aplican a descubrimientos basados en script.

Fix Pack 4 **com.ibm.cdb.discover.enableOutputFileSplittingProcess=true**

El valor predeterminado es `true`.

Esta propiedad especifica si el archivo de salida principal se ha creado durante un descubrimiento basado en scripts se divide en archivos más pequeños. El archivo se divide de forma predeterminada. Esta configuración impide que se produzcan problemas de rendimiento cuando el archivo de salida es grande. Consulte también la propiedad `com.ibm.cdb.discover.numberOfLinesForOutputFileSplittingProcess`.

Fix Pack 4

com.ibm.cdb.discover.numberOfLinesForOutputFileSplittingProcess=10000

El valor predeterminado es `10000`.

Esta propiedad se habilita solo cuando la propiedad `com.ibm.cdb.discover.enableOutputFileSplittingProcess` se establece en `true`.

Esta propiedad especifica que el número aproximado de líneas permitidas en los archivos de salida más pequeños, que se crearon dividiendo el archivo de salida principal. El formato de archivo determina el número exacto de líneas. Después del número de líneas especificado, el archivo se divide solo cuando se alcanza el final del conjunto significativo de datos para garantizar que todo el formato de archivo es correcto. Significa que cuando el valor se establece en `10000`, los archivos más pequeños pueden tener, por ejemplo, 10200 líneas.

com.ibm.cdb.taddm.asd.prefix=sh
El valor predeterminado es `sh`.

Esta propiedad especifica un prefijo que añadir al script que se ejecuta durante un descubrimiento, por ejemplo, *prefijo* `script.sh`. Esta propiedad es una propiedad con ámbito; puede añadir una dirección IP o el nombre de un conjunto de ámbitos.

com.ibm.cdb.discover.DeleteScriptDiscoveryOutputs=true
El valor predeterminado es `true`.

Esta propiedad especifica si se debe eliminar la salida del script que, durante el descubrimiento basado en script, se copia al servidor de TADDM para su procesamiento por los sensores. Esta salida podría resultar útil para la resolución de problemas, de forma predeterminada, se elimina después de que se completa el descubrimiento. Si se define el valor de esta propiedad en `false`, no se eliminará la salida del script.

com.ibm.cdb.discover.DeleteRemoteBeforeScriptsRun=false
El valor predeterminado es `false`.

Esta propiedad especifica si TADDM elimina las salidas que deja el descubrimiento anterior del directorio remoto antes de intentar ejecutar un nuevo descubrimiento.

com.ibm.cdb.discover.PreferScriptDiscovery=false
El valor predeterminado es `false`.

Esta propiedad se utiliza para habilitar el descubrimiento basado en script y afecta sólo a los sensores que soportan el descubrimiento basado en script. Al definir el valor en `true` se habilita el descubrimiento basado en script.

com.ibm.cdb.discover.smallFileSizeLimit=1048576
El valor predeterminado es `1048576` (1024*1024 - 1 MB).

Esta propiedad define el límite de tamaño de archivo expresado en bytes para operaciones de copia que desencadena el uso de sumas de comprobación. Los archivos cuyo tamaño está por debajo de este límite se copian sin los cálculos de suma de comprobación. Los archivos cuyo tamaño es igual o mayor que el límite sólo se copian si no están presentes en el directorio de destino y su suma de comprobación no coincide con el archivo local (origen).

Puede inhabilitar el límite utilizando los valores siguientes:

- `0`: la operación de copia siempre utiliza la suma de comprobación.
- `-1`: la operación de copia siempre evita utilizar la suma de comprobación

Propiedades del descubrimiento mediante IBM Tivoli Monitoring (método antiguo):

Estas propiedades se aplican al descubrimiento mediante IBM Tivoli Monitoring (método antiguo).

Método de integración antiguo

Esta sección está dedicada a un método en desuso de la integración de TADDM con IBM Tivoli Monitoring. A partir de la versión 7.3.0 de TADDM se recomienda efectuar la integración con IBM Tivoli Monitoring 6.3 mediante la automatización de OSLC. El método antiguo de la integración con el uso del sensor de IBM Tivoli Monitoring Scope está en desuso y se eliminará en los próximos releases. Para obtener más información sobre las propiedades utilizadas para configurar el proceso de descubrimiento mediante la automatización de OSLC, consulte "Integración de TADDM con IBM Tivoli Monitoring mediante la automatización de OSLC" en la página 201 y "Propiedades para el descubrimiento utilizando la sesión de automatización de OSLC" en la página 86.

Propiedades que afectan cómo TADDM descubre los puntos finales de Tivoli Monitoring

El descubrimiento TADDM de nivel 2 y nivel 3 generalmente requiere un servidor de dominio (en un despliegue de servidor de sincronización o de dominio) o un servidor de descubrimiento (en un despliegue de modalidad continua) para conectarse directamente a un sistema de destino utilizando uno de los métodos siguientes:

- Secure Shell (SSH) para sistemas de destino basados en UNIX
- Windows Management Instrumentation (WMI) para sistemas Windows

Para utilizar estos métodos, el servidor de dominio o de descubrimiento debe saber cómo utilizar las credenciales de usuario (cuenta y contraseña).

El descubrimiento mediante IBM Tivoli Monitoring permite a TADDM descubrir información del nivel 2 (y alguna del nivel 3) acerca de los sistemas de destino para los que no hay credenciales de usuario disponibles. Los sensores se ejecuten mediante la infraestructura de Tivoli Monitoring y únicamente son necesarias las credenciales de Tivoli Enterprise Portal Server. Después de configurar el sensor IBM Tivoli Monitoring Scope y ejecutarlo, los próximos descubrimientos de nivel 2 utilizan de forma predeterminada Tivoli Monitoring para el descubrimiento. Dado que es posible que no desee este comportamiento predeterminado en su entorno, TADDM proporciona las siguientes propiedades del servidor para controlar si se utiliza para el descubrimiento la conexión de Tivoli Monitoring o la conexión directa (SSH o WMI). Estas propiedades se pueden establecer en el nivel global o para un ámbito o perfil de descubrimiento específico.

com.ibm.cdb.session.allow.ITM=true

El valor predeterminado es `true`, lo que significa que TADDM puede utilizar IBM Tivoli Monitoring para descubrir los puntos finales de Tivoli Monitoring.

Esta propiedad especifica si TADDM puede utilizar IBM Tivoli Monitoring para descubrir los puntos finales de Tivoli Monitoring.

Para conectar directamente con un punto final de Tivoli Monitoring, establezca el valor en `false`.

También puede utilizar esta propiedad para especificar un ámbito de descubrimiento personalizado, como se indica en el ejemplo siguiente:

com.ibm.cdb.session.allow.ITM.*dirección_ip*=false
El ejemplo siguiente especifica que TADDM utiliza el ámbito de descubrimiento 10.20.30.40 y se conecta directamente con el punto final, incluso si lo supervisa Tivoli Monitoring:

```
com.ibm.cdb.session.allow.ITM.10.20.30.40=false
```

com.ibm.cdb.session.prefer.ITM=true
El valor predeterminado es true, que significa que TADDM utiliza IBM Tivoli Monitoring para descubrir los puntos finales de Tivoli Monitoring.

Esta propiedad especifica si TADDM utiliza IBM Tivoli Monitoring como método preferido para descubrir puntos finales de Tivoli Monitoring, presuponiendo que se permite el descubrimiento mediante IBM Tivoli Monitoring para puntos finales. Si TADDM utiliza IBM Tivoli Monitoring para el descubrimiento y el descubrimiento no es satisfactorio, TADDM utiliza una conexión directa con los puntos finales. Del mismo modo, si el descubrimiento mediante IBM Tivoli Monitoring no es el método preferido y la conexión directa con el punto final no es satisfactoria, TADDM intenta conectar con los puntos finales utilizando IBM Tivoli Monitoring, presuponiendo, una vez más, que se permite el descubrimiento mediante IBM Tivoli Monitoring para los puntos finales.

También puede utilizar esta propiedad para especificar un ámbito de descubrimiento personalizado, como se indica en el ejemplo siguiente:

com.ibm.cdb.session.prefer.ITM.*dirección_ip*=false
El ejemplo siguiente especifica que TADDM utiliza el ámbito de descubrimiento 10.20.30.40 y se conecta directamente con los puntos finales de Tivoli Monitoring:

```
com.ibm.cdb.session.prefer.ITM.10.20.30.40=false
```

com.ibm.cdb.session.prefer.ITM.Level_3_Discovery=false
El valor predeterminado es false, lo que significa que TADDM se conecta directamente con los puntos finales de Tivoli Monitoring si utiliza un perfil de descubrimiento de nivel 3, pero para todos los otros niveles de descubrimiento, TADDM utiliza IBM Tivoli Monitoring para descubrir los puntos finales de Tivoli Monitoring, en función de las siguientes propiedades:

- **com.ibm.cdb.session.allow.ITM**
- **com.ibm.cdb.session.prefer.ITM**

Esta propiedad especifica si TADDM utiliza IBM Tivoli Monitoring para descubrir los puntos finales de Tivoli Monitoring si utiliza un perfil de descubrimiento de nivel 3.

Si establece el valor en true, TADDM puede utilizar IBM Tivoli Monitoring para descubrir los puntos finales de Tivoli Monitoring desde un perfil de descubrimiento de nivel 3.

Propiedades de ajuste de la conexión entre el servidor TADDM y el servidor del portal

Para un descubrimiento de IBM Tivoli Monitoring de nivel 3, TADDM utiliza las siguientes propiedades del servidor TADDM para ajustar el comportamiento de recuperación de la conexión, si se cuelga la conexión entre el servidor TADDM y Tivoli Enterprise Portal Server:

com.collation.discover.agent.ITM.CmdWrapperSelectionPattern=
Esta propiedad especifica los mandatos que se deben envolver en un script cuando se ejecuta un descubrimiento mediante un entorno IBM Tivoli Monitoring.

com.collation.platform.session.ITMSessionConnectionCooldownPeriod=60000
Esta propiedad especifica el intervalo de tiempo en milisegundos que es necesario esperar a que la conexión a Tivoli Enterprise Portal Server se reinicialice después de haber detectado una anomalía.

com.collation.platform.session.ITMSessionConnectionRetryLimit=5
Esta propiedad especifica el número de veces que se ha de intentar acceder a la conexión si falla la conexión inicial, antes de informar acerca de un error.

com.collation.platform.session.ITMSessionNumProgressChecks=600
Esta propiedad especifica el número de veces que se comprueba el progreso de una conexión antes de que falle la conexión.

com.collation.platform.session.ITMSessionProgressCheckInterval=1000
Esta propiedad especifica el intervalo de tiempo en milisegundos entre cada comprobación del progreso de la conexión.

Propiedades para el descubrimiento utilizando la sesión de automatización de OSLC:

Estas propiedades se aplican al descubrimiento utilizando la sesión de automatización de OSLC.

Propiedades relacionadas con la integración a través de OSLC

com.ibm.cdb.topobuilder.integration.oslc.automationprovider
Esta propiedad especifica las direcciones URL directas de los proveedores de servicios de automatización de ejecución de OSLC que no están registrados en los servicios de registro de Jazz SM.

El ejemplo siguiente muestra las direcciones URL del proveedor de servicios de automatización de ejecución de OSLC para ITM:

```
com.ibm.cdb.topobuilder.integration.oslc.automationprovider=
http://<AUTOMATION_PROVIDER_INSTALLATION_HOST>:15210/itmautomationprovider
```

El ejemplo siguiente muestra cómo especificar las direcciones URL para varios proveedores de servicios de automatización de ejecución de OSLC:

```
com.ibm.cdb.topobuilder.integration.oslc.automationprovider.1=
http://9.1.1.1:15210/itmautomationprovider
com.ibm.cdb.topobuilder.integration.oslc.automationprovider.2=
http://9.2.2.2:15210/itmautomationprovider
```

com.ibm.cdb.topobuilder.integration.oslc.automation.scope.alwaysrefresh=false
El valor predeterminado es `false`.

Esta propiedad es una propiedad global que especifica si OSLCAutomationAgent vuelve a crear conjuntos de ámbitos durante cada ejecución. Para volver a crear los conjuntos de ámbitos, necesita una conexión a los servicios de registro de Jazz SM o a los proveedores de servicios de automatización de ejecución de OSLC, o a ambos.

Si la propiedad se establece en `true`, el agente vuelve a crear los conjuntos de ámbitos, aunque el plan de automatización proporcionado por el proveedor de servicios de automatización de ejecución de OSLC no haya cambiado desde la última ejecución del agente.

com.ibm.cdb.topobuilder.integration.oslc.frsurl
Esta propiedad especifica la dirección IP de servicios de registro de Jazz SM (FRS) que se utiliza para la integración con otros productos a través de OSLC. La dirección de los servicios de registro de Jazz SM debe tener el siguiente formato:

`protocol://ip_o_nombre_host:puerto`

OSLCAgent también utiliza esta propiedad.

com.ibm.cdb.topobuilder.integration.oslc.automation.frsurl
Esta propiedad especifica la dirección IP con una vía de acceso completa del conjunto de registros de los servicios de registro de Jazz SM (FRS). Puede utilizarse cuando los servicios de registro de Jazz SM utilizan otra vía de acceso de servicios distinta de la predeterminada, `/oslc`.

Propiedades relacionadas con el descubrimiento utilizando la sesión de automatización

com.ibm.cdb.session.oslcautomation.pluginId=com.ibm.cdb.session.oslcautomation_1.0.0
El valor predeterminado es `com.ibm.cdb.session.oslcautomation_1.0.0`.

Esta propiedad especifica el id de paquete OSGi del plug-in de sesión de automatización de OSLC.

com.ibm.cdb.session.itm.endpointClass=com.collation.platform.session.oslcautomation.OSLCAutomationEndpoint
El valor predeterminado es `com.collation.platform.session.oslcautomation.OSLCAutomationEndpoint`.

Esta propiedad especifica la clase de punto final que se va a utilizar.

com.ibm.cdb.session.allow.OSLCAutomation=true
El valor predeterminado es `true`.

Esta propiedad es una propiedad con ámbito que especifica si TADDM puede utilizar la sesión de automatización de OSLC durante el descubrimiento.

Ejemplo de uso:

```
com.ibm.cdb.session.allow.OSLCAutomation=true
com.ibm.cdb.session.allow.OSLCAutomation.9.100.1.0=true
com.ibm.cdb.session.allow.OSLCAutomation.scope_set2=true
```

com.ibm.cdb.session.prefer.OSLCAutomation=true
El valor predeterminado es `true`.

Esta propiedad es una propiedad con ámbito que especifica si la sesión de automatización de OSLC es una sesión preferida para un descubrimiento. El valor de esta propiedad tiene prioridad sobre otros valores preferidos, por ejemplo, una sesión ITM estándar.

Ejemplo de uso:

```
com.ibm.cdb.session.prefer.OSLCAutomation=true
com.ibm.cdb.session.prefer.OSLCAutomation.9.100.100.200=true
com.ibm.cdb.session.prefer.OSLCAutomation.scope_name1=true
```

com.ibm.cdb.session.oslcautomation.timeout.httpconnect=60000
El valor predeterminado es `60000` (60 segundos). El valor se expresa en milisegundos.

Esta propiedad es una propiedad global que especifica el tiempo de espera de la conexión con el proveedor de servicios de automatización de ejecución de OSLC.

com.ibm.cdb.session.oslcautomation.timeout.httpread=240000
El valor predeterminado es `240000` (4 minutos). El valor se expresa en milisegundos.

Esta propiedad es una propiedad global que especifica el tiempo de espera para leer los datos del proveedor de servicios de automatización de ejecución de OSLC.

com.ibm.cdb.session.oslcautomation.request.async.maxretries=60
El valor predeterminado es `60`.

Esta propiedad es una propiedad global que especifica el número máximo de solicitudes consecutivas de AutomationResults generados de forma asíncrona.

com.ibm.cdb.session.oslcautomation.request.async.delay=10000
El valor predeterminado es `10000` (10 segundos). El valor se expresa en milisegundos.

Esta propiedad es una propiedad global que especifica el tiempo de retardo entre solicitudes consecutivas de AutomationResults generados de forma asíncrona.

Nota: Fix Pack 4 En caso de que la sesión SSH para el servidor falle debido a problemas de tiempo de espera, intente configurar un valor óptima para la propiedad siguiente:

com.collation.mindterm.Ssh2Preferences= hello-timeout=30; alive = 25; compression= 9

com.collation.discover.agent.app.packagedapp.mysap.SLDServerPortList = 51200
Esta propiedad permite cambiar el puerto SLD y el puerto especificado se debe añadir en la configuración del sensor.

com.ibm.cdb.security.auth.cache.itm.disabled=true
El valor predeterminado es `true`.

Esta propiedad determina si está inhabilitado el almacenamiento en memoria caché de las credenciales para el descubrimiento de OSLC.

Esta propiedad es una propiedad con ámbito y perfil. Puede añadir una dirección IP, el nombre de un conjunto de ámbitos o un nombre de perfil. También puede establecerla en la configuración del perfil en la consola de Discovery Management.

Propiedades de personalización de búsqueda DNS

Estas propiedades se aplican a la personalización de búsquedas de DNS.

com.collation.platform.os.disableDNSLookups=false
El valor predeterminado es `false`.

Los valores válidos son `true` o `false`. Si cambia la propiedad a `true`, las búsquedas de DNS se inhabilitan para el servidor TADDM.

com.collation.platform.os.disableRemoteHostDNSLookups=false
El valor predeterminado es `false`.

Los valores válidos son `true` o `false`. Si cambia la propiedad a `true`, las búsquedas de nombres (por ejemplo JAVA y DNS) están inhabilitadas en

hosts descubiertos remotos. Esta propiedad obliga a que todas las búsquedas de nombres tengan lugar en el servidor de TADDM.

com.collation.platform.os.command.fqdn=nslookup $1 | grep Name | awk '{print $2}'

El valor predeterminado es `nslookup $1 | grep Name | awk '{print $2}'`.

Este mandato se utiliza para buscar el nombre completo de dominio (fqdn). En la mayoría de las situaciones, esta propiedad no es necesaria porque el algoritmo de nombre completo de dominio totalmente calificado (FQDN) predeterminado funciona en la mayoría de los entornos de producción. Si esta propiedad no es necesaria, debe marcarla como comentario. No obstante, en entornos en los que el nombre completo de dominio debe derivar del nombre de host, es posible habilitar esta propiedad. Por ejemplo, habilite esta propiedad si los nombres de host están configurados como alias en DNS.

Si utiliza esta propiedad, asegúrese de que DNS esté disponible y la propiedad configurada. De lo contrario, es posible que el mandato **nslookup** no se ejecute correctamente o tenga un tiempo de respuesta lento.

Si está habilitada, esta propiedad sólo se utiliza en el servidor de TADDM. Actualmente, solo son compatibles los sistemas operativos AIX y Linux. Esta propiedad no se soporta en el servidor de TADDM de Windows.

Propiedades de la interfaz gráfica de usuario

Estas propiedades se aplican a la interfaz gráfica de usuario de TADDM.

Fix Pack 3 **com.ibm.cdb.gui.supportedJRE.warning=true**

Esta propiedad especifica si se debe visualizar el mensaje de aviso CTJTG0034E cuando se inicia la Consola de gestión de descubrimiento. Este mensaje avisa de que posee una versión no soportada del entorno de tiempo de ejecución de Java. Si desea utilizar TADDM con la versión no soportada del entorno de tiempo de ejecución de Java, y no desea que se visualice este mensaje, establezca esta propiedad en `false`.

El valor predeterminado de esta propiedad es `true`.

Propiedades de memoria de la máquina virtual Java de la interfaz gráfica de usuario:

Estas propiedades se aplican a la memoria de la máquina virtual Java de la interfaz gráfica de usuario.

com.collation.gui.initial.heap.size=128m

El valor predeterminado es `128m`.Tamaño de almacenamiento dinámico inicial para la interfaz de usuario de TADDM.

com.collation.gui.max.heap.size=512m

El valor predeterminado es `512m`.Tamaño máximo de almacenamiento dinámico para la interfaz de usuario de TADDM.

Estas propiedades son adecuadas para un dominio de TADDM pequeño. Para fines de dimensionamiento, se utilizan las siguientes categorías de servidores de TADDM (de acuerdo con los equivalentes de servidor):

- Pequeño: hasta 1000 equivalentes de servidor
- Mediano: 1000 a 2500 equivalentes de servidor
- Grande: 2500 a 5000 equivalentes de servidor

Aumentar estos valores para entornos medianos y grandes mejora el rendimiento para algunas operaciones de GUI. Algunas vistas no se completan correctamente si no hay suficiente memoria disponible para TADDM en el momento de la acción.

Para un entorno mediano:

com.collation.gui.initial.heap.size=256m

El valor predeterminado es 256m.

com.collation.gui.max.heap.size=768m

El valor predeterminado es 768m.

Para un entorno grande:

com.collation.gui.initial.heap.size=512m

El valor predeterminado es 512m.

com.collation.gui.max.heap.size=1024m

El valor predeterminado es 1024m.

Propiedades del puerto de interfaz gráfica de usuario (GUI):

Estas propiedades se aplican a los puertos de GUI.

com.collation.tomcatshutdownport=9436 (solo TADDM 7.3.0)
El valor predeterminado es 9436.

Este puerto se utiliza para el mandato de cierre de Tomcat.

com.ibm.cdb.service.web.port=9430
El valor predeterminado es 9430.

El puerto HTTP se utiliza sin SSL.

com.ibm.cdb.service.web.secure.port=9431
El valor predeterminado es 9431.

El puerto HTTPS se utiliza con SSL.

com.ibm.cdb.service.ClientProxyServer.port=9435
El valor predeterminado es 9435.

El puerto de datos RMI que hay que utilizar sin SSL.

com.ibm.cdb.service.SecureClientProxyServer.secure.port=9434
El valor predeterminado es 9434.

El puerto de datos RMI que hay que utilizar con SSL.

com.ibm.cdb.service.registry.public.port=9433
El valor predeterminado es 9433.

El puerto de registro de servicio público.

Propiedades de LDAP

Estas propiedades se aplican a LDAP.

Se puede utilizar un servidor LDAP externo para la autenticación de usuarios. Mediante un servidor LDAP externo, se puede dar soporte a la autenticación anónima o a la basada en contraseña.

El nombre de host del servidor LDAP, el número de puerto, el nombre distinguido básico, el nombre distinguido bind y la contraseña (necesaria para la autenticación basada en contraseña) se pueden configurar en el archivo `collation.properties`. También puede configurar el atributo de denominación específico que se puede buscar para que coincida con el ID de usuario (UID).

La configuración de LDAP está recomendada en los despliegues de servidores de sincronización y de dominio. En un entorno empresarial, configure el servidor de dominio y el servidor de sincronización para utilizar el mismo registro de usuario. Cuando inicie sesión en un servidor de dominio conectado a un servidor de sincronización, se procesará el inicio de sesión en el servidor de sincronización. Si se produce un problema de conexión de red entre el servidor de sincronización y el servidor de dominio, se puede iniciar sesión correctamente en el servidor de dominio sin la reconfiguración siempre que el servidor de dominio esté configurado para utilizar el mismo registro de usuario que el servidor de sincronización.

com.collation.security.auth.ldapAuthenticationEnabled=true
El valor predeterminado es `true`.

Esta propiedad se utiliza para habilitar la autenticación LDAP.

com.collation.security.auth.ldapBaseDN=ou=People,dc=ibm,dc=com
El valor predeterminado es `ou=People,dc=ibm,dc=com`.

Esta propiedad define el nombre distinguido básico de LDAP (DN). El Nombre distinguido básico de LDAP es el punto inicial de todas las búsquedas de LDAP.

com.collation.security.auth.ldapBaseGroupDN
En el archivo `collation.properties`, esta propiedad está comentada de forma predeterminada.

Esta propiedad define la ramificación raíz de LDAP para los grupos de búsqueda, que pueden ser diferentes de la ramificación raíz de todas las consultas de LDAP. Para especificar más de una rama raíz de LDAP para buscar grupos, separe los nombres de las ramas mediante el carácter ";".

Si no se especifica ningún valor para esta propiedad, el valor predeterminado es el valor de la propiedad `com.collation.security.auth.ldapBaseDN`.

com.collation.security.auth.ldapBindDN=uid=ruser,dc=ibm,dc=com
El valor predeterminado es `uid=ruser,dc=ibm,dc=com`.

Si se utiliza la autenticación simple, esta propiedad define el ID de usuario que se utiliza para autenticarse en LDAP.

Importante:

- Si no se ha proporcionado `com.collation.security.ldapBindDN` o si la propiedad está marcada como comentario, se intenta una conexión anónima con LDAP. El ejemplo siguiente muestra cómo se puede marcar como comentario la propiedad con el signo de almohadilla (#):

  ```
  #com.collation.security.auth.ldapBindDN=uid=ruser,
  dc=ibm,dc=com
  ```

- Si se ha especificado un valor para `com.collation.security.auth.ldapBindDN`, se utiliza la autenticación simple y
- y también debe especificarse un valor para `com.collation.security.auth.ldapBindPassword`.

com.collation.security.auth.ldapBindPassword=ruser
El valor predeterminado es `ruser`.

Si se utiliza la autenticación simple, esta propiedad define la contraseña de usuario que se utiliza para autenticarse en LDAP.

com.collation.security.auth.ldapClientKeyStore=*vía_acceso_ks*
La propiedad define la ubicación del almacén de claves que contiene los certificados en el servidor de TADDM. El almacén debe contener el certificado de cliente para autenticar el servidor de TADDM con el servidor LDAP.

com.collation.security.auth.ldapClientKeyStorePassphrase=*frase_contraseña_ks*
Opcional: esta propiedad define la contraseña para el almacén de claves.

com.collation.security.auth.ldapClientTrustStore=*vía_acceso_ts*
La propiedad define la ubicación del almacén de confianza que contiene los certificados en el servidor de TADDM. El almacén debe contener el certificado del servidor LDAP.

com.collation.security.auth.ldapClientTrustStorePassphrase=*frase_contraseña_ts*
Opcional: esta propiedad define la contraseña para el almacén de confianza.

com.collation.security.auth.ldapGroupMemberAttribute=member
El valor predeterminado es `member`.

Esta propiedad define el nombre del atributo que se utiliza para contener los miembros de un grupo en LDAP.

com.collation.security.auth.ldapGroupNamingAttribute=cn
El valor predeterminado es `cn`.

Esta propiedad define el nombre del atributo que se utiliza para la asignación de nombres de grupos en LDAP.

com.collation.security.auth.ldapGroupObjectClass=grupofnames
El valor predeterminado es `grupo_de_nombres`.

Esta propiedad define la clase utilizada para representar a grupos de usuarios en LDAP.

com.collation.security.auth.ldapHostName=ldap.ibm.com
El valor predeterminado es `ldap.ibm.com`.

Esta propiedad define el nombre de host para el servidor LDAP.

com.collation.security.auth.ldapPortNumber=389
El valor predeterminado es `389`.

Esta propiedad define el puerto para el servidor LDAP.

com.collation.security.auth.ldapUIDNamingAttribute=uid
El valor predeterminado es `uid`.

Esta propiedad define el nombre del atributo que se utiliza para la asignación de nombres de usuarios en LDAP.

com.collation.security.auth.ldapUserObjectClass=person
El valor predeterminado es `person`.

Esta propiedad define el nombre de la clase que se utiliza para representar a usuarios en LDAP.

com.collation.security.auth.ldapUseSSL=false
El valor predeterminado es `false`.

La propiedad se utiliza para habilitar la autenticación para un registro de usuario LDAP mediante una conexión SSL.

com.collation.security.usermanagementmodule=ldap
El valor predeterminado es `ldap`.

Esta propiedad define el módulo de gestión de usuarios que el servidor de TADDM utiliza. Los valores válidos son:

- `file` para un registro de usuario basado en archivo. El valor predeterminado es true.
- `ldap` para un registro de usuario de LDAP
- `vmm` para un registro que utiliza repositorios federados de WebSphere Application Server

Propiedades de bloqueo

Estas propiedades se aplican a los bloqueos.

com.collation.security.lockout.treshold=3
El valor predeterminado es `3`.

Esta propiedad especifica el número de intentos de inicio de sesión fallidos, para un usuario concreto, que desencadena un bloqueo local para dicho usuario.

com.collation.security.lockout.timeout=30
El valor predeterminado es `30`.

Esta propiedad especifica el tiempo, en minutos, durante el que el usuario que ha activado el bloqueo local está desconectado por seguridad de TADDM, cuando se activa un bloqueo local.

com.collation.security.lockout.globalthreshold=100
El valor predeterminado es `100`.

Esta propiedad especifica el número de bloqueos simultáneos de usuarios individuales que desencadena un bloqueo global.

com.collation.security.lockout.globaltimeout=30
El valor predeterminado es `30`.

Esta propiedad especifica el tiempo, en minutos, durante el que todos los usuarios están desconectados por seguridad de TADDM, cuando se activa un bloqueo global.

com.collation.security.lockout.failedloginthreshold=1000
El valor predeterminado es `1000`.

Esta propiedad especifica el número total de intentos de inicio de sesión fallidos para usuarios individuales que desencadena un bloqueo global.

Propiedades de registro

Estas propiedades se aplican al registro.

com.collation.log.filesize=20MB
El valor predeterminado es `20MB`.

El tamaño máximo del archivo de registro. Cuando el archivo alcanza este límite de tamaño, se crea un archivo de registro nuevo. El archivo de registro actual se guarda con la extensión de archivo **.***N*. *N* es el número 1 en el conjunto de valores de la propiedad **com.collation.log.filecount**. Establece cuántos archivos de registro puede crear y guardar antes de que los archivos roten con la propiedad **com.collation.log.filecount**.

Puede especificar el número de bytes directamente o especificar el número de kilobyte o megabyte utilizando KB y MB respectivamente.

Los ejemplos siguientes son valores de tamaño de archivo de registro válidos:

- 1000000
- 512 KB
- 10 MB

com.collation.log.filecount=5
El valor predeterminado es 5.

El número de archivos de registro que mantiene.

com.collation.log.level.vm.*NombreMáquinaVirtual*=INFO
El valor predeterminado es INFO

Establece el nivel de registro para cada sistema virtual.

NombreMV es el sistema virtual de Java asociado al nombre del servicio de TADDM. La lista siguiente identifica otras opciones válidas:

- Topología
- DiscoverAdmin
- EventsCore
- Proxy
- Discover
- EcmdbCore
- StorageService
- DiscoveryService

La lista siguiente identifica otras opciones válidas:

- MUY GRAVE
- ERROR
- AVISO
- INFO
- DEPURACIÓN (Al establecer la opción DEPURACIÓN disminuye el rendimiento del sistema.)
- RASTREO (La opción RASTREO hace que se registren las contraseñas.)

Propiedades de rendimiento

Estas propiedades se aplican al rendimiento de TADDM.

com.collation.discover.dwcount=32
El valor predeterminado es 32. El valor debe ser un valor entero.

Esta propiedad influye en la velocidad de descubrimiento. Una hebra Worker de descubrimiento es una hebra que ejecuta sensores. Esta propiedad especifica cuantas hebras Worker de descubrimiento se pueden ejecutar a la vez, y solo se aplica a un servidor de descubrimiento en un despliegue de servidor de modalidad continua o a un servidor de dominio en un despliegue de servidor de dominio.

Para efectuar un descubrimiento mediante IBM Tivoli Monitoring (método antiguo que utiliza el sensor de IBM Tivoli Monitoring Scope), el valor debe ser 16. Para los demás tipos de descubrimiento, el rango válido de valores es de 32 a 160.

com.collation.discover.observer.topopumpcount=16
El valor predeterminado es 16. El valor debe ser un valor entero.

Esta propiedad influye en la velocidad a la que se almacenan los resultados del descubrimiento en la base de datos de TADDM. Especifica el número de hebras de grabador que se crean para comunicarse con la base de datos de TADDM.

En el caso de un servidor de descubrimiento en un despliegue de servidor en modalidad continua, la propiedad controla el número de hebras que el servidor de descubrimiento utiliza para enviar los resultados del descubrimiento a la agrupación de servidores de almacenamiento.

En el caso de un servidor de almacenamiento en un despliegue de servidor en modalidad continua, la propiedad controla el número de hebras que reciben resultados del descubrimiento de los servidores de descubrimiento.

En el caso de un servidor de dominio en un despliegue de servidor de dominio, esta propiedad controla el número de hebras que reciben resultados del descubrimiento de las hebras Worker de descubrimiento.

Luego las hebras utilizan una conexión de base de datos de la agrupación de conexiones para comunicarse con la base de datos de TADDM (por ejemplo, para almacenar resultados y recuperar datos). Si no hay más conexiones agrupadas de JDBC, la hebra crea una conexión no agrupada.

com.ibm.cdb.discover.observer.topopump.threshold=0.7
com.ibm.cdb.discover.observer.topopump.threshold.*grupo_agente_topol*=0.7
El valor predeterminado es 0.7. El valor debe ser una constante flotante.

Esta propiedad especifica la fracción de las hebras de grabador de la base de datos que puede iniciar cuando los agentes de topología estén en ejecución. Puede especificar el valor de umbral de forma independiente para un grupo de agentes determinado o para todos ellos a la vez. Si el valor no está definido para un grupo de agentes, se utiliza el valor de umbral general. Este valor permite la limitación de hebras que almacenan los resultados del descubrimiento en la base de datos de TADDM cuando los agentes de topología se ejecutan .

com.ibm.cdb.typesServiceRefreshInterval=120
El valor predeterminado es 120. El valor mínimo es 30, mientras que el máximo es 1800.

Esta propiedad especifica, en segundos, el intervalo de renovación para actualizar los tipos de componentes al crear una consulta personalizada, mostrar un historial de cambios o visualizar información de comparación de componentes.

com.ibm.cdb.ea.metaRefreshFrequency=20
El valor predeterminado es 20. El valor debe ser un valor entero.

Esta propiedad especifica, en segundos, el intervalo de actualización para actualizar la información sobre los atributos ampliados definidos, por ejemplo, en los servidores de almacenamiento.

Propiedades de Secure Shell (SSH)
Estas propiedades se aplican a Secure Shell (SSH).

Fix Pack 1 **com.ibm.cdb.platform.SshVersionSessionSkipList**
Esta propiedad especifica las versiones de los servidores SSH para los cuales no se ha establecido la sesión. En el caso de dichos servidores, el sensor de sesión se finaliza sin errores.

El valor de esta propiedad es una lista separada por comas, por ejemplo `Cisco,Data ONTAP,SSH-2.0-OpenSSH_5.9 PKIX FIPS,OpenSSH_OA`.

com.collation.SshLogInput=false
El valor predeterminado es `false`.

Los valores válidos son `true` o `false`. Si establece el valor en `true`, se registra la entrada SSH.

com.collation.SshPort=22
El valor predeterminado es `22`. El valor debe ser un valor entero.

Esta propiedad indica el puerto que el servidor utiliza para todas las conexiones SSH.

com.collation.SshSessionCommandTimeout=120000
El valor predeterminado es `120000`. El valor debe ser un valor entero.

Este valor indica el tiempo (en milisegundos) que se permite para que se ejecute el mandato SSH. Para que sea efectiva si esta propiedad se utiliza desde un agente, el valor para esta propiedad debe ser menor que el valor para que la propiedad **AgentRunnerTimeout**.

com.collation.SshWeirdReauthErrorList=Permiso denegado

Esta propiedad permite el reintento del par de nombre de usuario y contraseña que han funcionado anteriormente durante las ejecuciones de descubrimiento. La propiedad es necesaria porque los sistemas Windows niegan de manera aleatoria los intentos de inicio de sesión válidos. La propiedad debe tener el valor `Permiso denegado`. No modifique esta propiedad.

com.collation.WmiInstallProviderTimeout=240000
El valor predeterminado es `240000`. El valor debe ser un valor entero.

Este valor indica el tiempo (en milisegundos) que se puede esperar hasta que se ejecuta el script WMI InstallProvider.

com.collation.SshSessionReuseSuppressList
Algunas versiones del servidor SSH no dan soporte a la reutilización de conexiones como implementadas por TADDM. Las versiones de servidor SSH que no están soportadas para su reutilización deben añadirse a esta propiedad para que TADDM descubra correctamente los destinos que ejecutan esas versiones de servidor SSH.

El valor de esta propiedad es una lista separada por comas. Es suficiente especificar sólo el principio de la versión del servidor SSH, por ejemplo, `SSH-2.0-BoKS_SSH_6`.

Puede encontrar la versión del servidor SSH en el archivo de registro del sensor de sesión.

Propiedades de seguridad

Estas propiedades se aplican a la seguridad.

Fix Pack 3 **com.ibm.cdb.secure.server=false**
El valor predeterminado es `false`.

Esta propiedad especifica si todos los servicios TADDM de los registros RMI públicos y externos están protegidos. Si se establece en `true`, todos los servicios públicos no protegidos (ClientProxyServer y servidor de API) se

moverán al registro RMI interno. Además, el protocolo SSL se aplica en servicios externos, por ejemplo, RegistriesURLProvider, SecurityManager y TopologyManager.

Si establece esta propiedad en `true`, defina también las propiedades `com.collation.security.enablesslforconsole` y `com.collation.security.enforceSSL` en `true`.

Esta propiedad podría afectar a la integración con otros productos que se conectan a TADDM con una conexión no segura.

Si modifica el valor predeterminado de esta propiedad, establézcalo en las siguientes ubicaciones:

- `$COLLATION_HOME/dist/etc/collation.properties`
- `$COLLATION_HOME/dist/sdk/etc/collation.properties`
- `sdk/etc/collation.properties` de cada instalación del SDK de TADDM.

Fix Pack 5 Si el servidor se ejecuta en modalidad segura (`com.ibm.cdb.secure.server = true`), el siguiente puerto se asegurará con el protocolo SSL:

- `com.ibm.cdb.service.registry.public.port (Valor predeterminado: 9433)`

Si el servidor se ejecuta en modalidad segura (`com.ibm.cdb.secure.server = true`), mientras se inicie la consola de gestión de datos, el recuadro de selección 'Establecer una sesión segura (SSL)' debe estar marcado.

Fix Pack 1 **com.ibm.cdb.secure.liberty=false**
El valor predeterminado es `false`.

Los valores válidos son `true` o `false`. Para inhabilitar el puerto HTTP no seguro, establezca este distintivo en `true`.

com.collation.security.privatetruststore=true
El valor predeterminado es `true`.

Los valores válidos son `true` o `false`. El valor debe ser `true` si SSL está habilitada.

com.collation.security.enablesslforconsole=true
El valor predeterminado es `true`.

Los valores válidos son `true` o `false`.

com.collation.security.enabledatalevelsecurity=false
El valor predeterminado es `false`.

Los valores válidos son `true` o `false`. Para restringir el acceso a las colecciones de objetos de TADDM por usuario o grupo de usuarios, establezca este valor en `true`.

com.collation.security.enforceSSL=false
El valor predeterminado es `false`.

Los valores válidos son `true` o `false`. Para inhabilitar las conexiones no seguras y forzar la utilización de conexiones SSL, establezca este distintivo en `true`.

com.collation.security.usermanagementmodule=archivo
El valor predeterminado es `file`.

Existen tres opciones para esta propiedad:

- `file` para un registro de usuario basado en archivo de TADDM

- `ldap` para un registro de usuario de LDAP
- `vmm` para un registro que utiliza repositorios federados de WebSphere Application Server

com.collation.security.auth.sessionTimeout=240
El valor predeterminado es `240`. El valor debe ser un valor entero.

com.collation.security.auth.searchResultLimit=100
El valor predeterminado es `100`. El valor debe ser un valor entero.

Utilice esta propiedad si tiene muchos usuarios.

Importante: Si tiene menos de 100 usuarios en un repositorio LDAP o un repositorio federado de WebSphere, incremente este valor para que dé soporte al número previsto de usuarios. Por ejemplo, `com.collation.security.auth.searchResultLimit=150`

com.collation.security.auth.websphereHost=hostlocal
El valor predeterminado es `localhost`.

Escriba el nombre completo de dominio del sistema que aloja la funcionalidad de repositorios federados de WebSphere Application Server.

com.collation.security.auth.websperePort=2809
El valor predeterminado es `2809`.

Debe ser un valor entero. Este valor indica el puerto del sistema WebSphere.

com.ibm.cdb.service.SecurityManager.port=9540
En el caso de servidores que no sean servidores de sincronización:

El valor predeterminado es `9540`.

Especifica el puerto del cortafuegos que utiliza el gestor de seguridad.

En el caso de un servidor de sincronización:
El valor predeterminado no está definido.
Los dominios se comunican con un servidor de sincronización utilizando un puerto que se especifica en el parámetro **`com.collation.EnterpriseSecurityManager.port`**. El valor predeterminado para esta propiedad es `19433`.

com.collation.cdm.analytics.authorizedRole=

El panel Analítica se puede restringir a un rol específico. De forma predeterminada, esta propiedad no está definida en el archivo `collation.properties` y el panel Analítica se encuentra disponible para todo el mundo. El valor de la propiedad debe ser el nombre del rol que está autorizado a acceder al panel.

El acceso a estas áreas del panel Analítica puede estar sujeto al rol especificado:

- Fix Pack 2 Patrones de agrupación
- Resumen de inventario
- Resumen de aplicaciones
- Resumen de servicio
- Inventario del sistema
- Inventario del servidor de software
- Informes BIRT

com.collation.security.discoverOutsideScope=true
El valor predeterminado es `true`.

Los valores válidos son `true` o `false`. Para inhabilitar los elementos de descubrimiento que no están dentro del ámbito, establezca este distintivo en `false`.

com.ibm.cdb.secure.tomcat=false (solo TADDM 7.3.0)
El valor predeterminado es `false`.

Los valores válidos son `true` o `false`. Para inhabilitar el puerto HTTP no seguro, establezca este distintivo en `true`.

com.ibm.cdb.http.ssl.protocol=TLS
El valor predeterminado es `TLS`.

Esta propiedad modifica el protocolo SSL que utiliza el puerto SSL web (puerto HTTPS), de manera predeterminada `9431`. Puede establecer el puerto mediante la propiedad `com.ibm.cdb.service.web.secure.port`.

Para ver la lista de valores soportados, consulte la documentación de IBM Java 7 en http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/protocols.html. Si utiliza los protocolos más seguros, por ejemplo, `TLS v1.1` o `TLS v1.2`, antes debe configurar el navegador web para que los admita. Asimismo, los protocolos demasiado estrictos pueden afectar a la integración con otros productos que se conectan a TADDM mediante el puerto SSL web.

Fix Pack 5 Cuando `com.ibm.cdb.http.ssl.protocol=TLSv1.2` y `JAVA7` se utiliza en el lado del cliente, se deben actualizar los siguientes valores:

```
<JAVA_HOME>/jre/lib/security/java.security
jdk.tls.disabledAlgorithms=SSLv2, SSLv3, TLSv1, TLSv1.1
```

Además, TLSv1 y TLSv1.1 deben estar inhabilitados en el navegador.

⌂**com.ibm.cdb.ssl.protocol=TLS**
Esta propiedad no está añadida al archivo `collation.properties` de forma predeterminada. Si no está añadida, el valor predeterminado será `TLS`. Para modificarlo, añada esta propiedad al archivo `collation.properties` manualmente con el valor nuevo.

Esta propiedad modifica el protocolo SSL que utilizan los puertos siguientes:

- El puerto de escucha del servidor de API para solicitudes SSL, de forma predeterminada `9531`. Puede establecer el puerto mediante la propiedad `com.ibm.cdb.service.SecureApiServer.secure.port`.
- El puerto de datos RMI que hay que utilizar con SSL, de forma predeterminada `9434`. Puede establecer el puerto mediante la propiedad `com.ibm.cdb.service.SecureClientProxyServer.secure.port`.

Para ver la lista de valores soportados, consulte la documentación de IBM Java 7 en http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/protocols.html. Si utiliza los protocolos más seguros, por ejemplo, `TLS v1.1` o `TLS v1.2`, antes debe configurar el navegador web para que los admita. Asimismo, los protocolos demasiado estrictos pueden afectar a la integración con otros productos que se conectan a TADDM mediante los puertos de la lista.

⌂**com.ibm.cdb.http.ssl.ciphers=**
Los cifrados se van a establecer en LibertyServer y la comunicación se realizará sólo en los cifrados proporcionados. De lo contrario, tomará los cifrados predeterminados que podrían ser los algoritmos débiles.

⌂**com.ibm.cdb.rmi.ssl.protocol=**
Esta propiedad `com.ibm.cdb.rmi.ssl.protocol` ayuda a habilitar un protocolo específico en la conexión SSL que se ha creado en `com.ibm.cdb.ssl.protocol`.

`com.ibm.cdb.rmi.ssl.protocol` debe ser de la lista de protocolos soportados en `com.ibm.cdb.ssl.protocol`.

⌂**com.ibm.cdb.rmi.ssl.ciphers=**
Con esta propiedad, puede establecer los algoritmos de cifrado para el puerto de datos de RMI y el puerto en el que escucha el servidor de API.

Propiedades del directorio temporal

Estas propiedades se aplican a directorios temporales.

Los directorios temporales los utiliza TADDM para almacenar archivos temporales en ciertas condiciones. Por ejemplo, los archivos de registro del ancla, los scripts de descubrimiento, los resultados de descubrimiento y la información que necesitan algunos sensores al ejecutar un descubrimiento pueden almacenarse en directorios temporales. TADDM utiliza tres directorios temporales: `ANCHOR_DIR`, `ASD_TEMP_DIR` y `TADDM_TEMP_ROOT`.

com.ibm.cdb.taddm.anchor.root=.
El valor predeterminado es `.\`.

Esta entrada especifica la ubicación del directorio `ANCHOR_DIR` donde se despliega el servidor ancla. Esta propiedad es una propiedad que está en el ámbito, y se le puede añadir la dirección IP, el nombre del ámbito o el sistema operativo. Por ejemplo, `com.ibm.cdb.taddm.anchor.root.SunOS=`.

Para un sistema Windows, se utilizan el siguiente nombre de propiedad y valor predeterminado:

```
com.ibm.cdb.taddm.anchor.root.Windows=%windir%\\temp\\
```

El valor de propiedad utiliza variables que se resuelve en los sistemas principales de destino. Las variables Linux, AIX y SunOS debe ir precedidas de un signo de dólar ($). Las variables de Windows deben ir incluidas entre signos de porcentaje (%). Por ejemplo, `com.ibm.cdb.taddm.anchor.root=$TMP/taddmdirs/anchor` y `com.ibm.cdb.taddm.anchor.root.Windows=%TEMP%\\taddmdirs\\anchor`.

Si el valor de propiedad resulto es una vía de acceso de directorio relativo, va precedida de:

- `%windir%\\temp\\` - en Windows
- Home directory - en sistemas AIX, Linux y SunOS

La vía de acceso va seguida del directorio `taddmversion/anchor`. Por ejemplo, `/home/taddmusr/taddm7.2.1/anchor` y `c:\Windows\Temp\taddm7.2.1\anchor`.

com.ibm.cdb.taddm.asd.temp
Esta entrada especifica la ubicación del directorio `ASD_TEMP_DIR` y este directorio almacena scripts y resultados de descubrimiento. Esta propiedad es una propiedad que está en el ámbito, y se puede personalizar añadiéndole la dirección IP o el sistema operativo.

En la ubicación especificada, se crea el directorio taddm*versión*/asd/. Por ejemplo, /tmp/taddm7.2.1/asd/. Si especifica una nueva ubicación, todos los usuarios debe tener todos los derechos de acceso a la nueva ubicación.

com.ibm.cdb.taddm.file.temp=.
El valor predeterminado es .\

Esta entrada especifica la ubicación de TADDM_TEMP_ROOT y este directorio lo utilizan varios sensores para almacenar datos temporales que son necesarios para ejecutar un descubrimiento. Algunos ejemplos de sensores que almacenan datos temporales son los sensores de DB2® y WebLogic.

El directorio TADDM_TEMP_ROOT se crea en el directorio de inicio en taddm*version*/temp/. Por ejemplo, /home/taddmusr/taddm7.2.1/temp/.

Propiedades del compilador de topologías

Estas propiedades se aplican al compilador de topologías.

com.collation.topobuilder.RuntimeGcUnknownServerRetentionSpan=5
El valor predeterminado es 5.

Esta propiedad especifica durante cuánto tiempo (en días) deben conservarse los procesos desconocidos. El valor máximo es 14. Los procesos desconocidos determinan cuándo son necesarias las plantillas de servidor. Sin embargo, sin una limpieza periódica, el número de procesos desconocidos puede acumularse con el tiempo. Esto puede causar problemas de rendimiento de topología. El elemento de espacio de direcciones de zOS no se elimina con este procesamiento.

com.collation.topobuilder.RuntimeGcThreadCount=
El valor predeterminado es 4.

Esta propiedad añade paralelismo al agente RuntimeGC, lo cual puede mejorar el rendimiento.

com.collation.topobuilder.agent.DerivedAppToAppDependencyAgent.ServiceDependency.enabled
El valor predeterminado es false.

Esta propiedad especifica si el agente de topología DerivedAppToAppDependency crea una dependencia entre las aplicaciones empresariales cuando sus miembros se encuentran en dependencia de servicio.

Para habilitar el agente a crear dicha dependencia, defina la propiedad en true.

Propiedades del gestor de topologías

Estas propiedades se aplican al gestor de topologías.

com.ibm.JdoQuery.FetchBatchSize=500
El valor predeterminado es 500.

El tamaño de proceso por lotes es una propiedad configurable y corresponde a la propiedad **kodo.FetchBatchSize**. Esta propiedad representa el número de filas que hay que captar simultáneamente al desplazarse por un conjunto de resultados de una ejecución de consulta.

com.ibm.cdb.service.TopologyManager.port=9550
El valor predeterminado es 9550.

Especifica el puerto del cortafuegos que utiliza el gestor de topologías.

Propiedades del gestor de vistas

Estas propiedades se aplican al gestor de vistas.

Fix Pack 2 **com.ibm.taddm.hideNetworkConnectionUnusedColumns.enabled**

El valor predeterminado es `false`.

Esta propiedad especifica si las siguientes columnas del separador **Conexiones de red** se muestran en el Portal de gestión de datos:

- **Flujos**
- **Paquetes**
- **Octetos**
- **Primera visualización**
- **Visualizado por última vez**

Para ocultar estas columnas, establezca esta propiedad en `true`.

com.collation.view.maxnodes=500

El valor predeterminado es `500`. El valor debe ser un valor entero.

Esta propiedad especifica el número máximo de nodos que se pueden visualizar en un gráfico de topologías en el portal de gestión de datos. Si establece la propiedad a un valor más elevado, puede ver topologías más amplias. Sin embargo, puede incrementar los requisitos de memoria.

Verificación de la integridad de los datos

Puede ejecutar el comando **`verify-data`** para verificar la integridad de los datos de los elementos de configuración de la base de datos TADDM. Puede verificar las relaciones, las correlaciones de herencias, los duplicados y las sobrefusiones.

Antes de empezar

No ejecute un descubrimiento, carga en bloque o sincronización con la opción de reparación habilitada. La herramienta de integridad de los datos analiza una gran cantidad de datos y el proceso puede tardar un tiempo, especialmente si se encuentra habilitada la opción de reparación. El servidor de TADDM debe estar activo y en ejecución, pero asegúrese de que no está efectuando ninguna tarea.

Acerca de esta tarea

La herramienta de verificación de integridad de los datos notifica y repara problemas de integridad de datos de los elementos de configuración de la base de datos TADDM. El script ejecutable se encuentra en el directorio `$COLLATION_HOME/bin`. La herramienta incluye los informes y registros en el archivo `verify-data.log`. Puede detener la herramienta y ejecutarla de nuevo siempre que lo desee.

Verificación de relaciones

La verificación de las relaciones consulta y verifica las claves foráneas en todas las tablas de modelos e intersecciones.

Acerca de esta tarea

Con la opción de reparación habilitada, la verificación de las relaciones suprime objetos hijo si no existe un objeto principal en la base de datos, y suprime claves foráneas no válidas para relaciones que se han definido como no contenidas. También puede suprimir un número significativo de elementos de configuración de

nivel inferior. Sin embargo, si los elementos no tienen un objeto principal, pueden suprimirse de forma segura.

Procedimiento

Para verificar las relaciones, ejecute uno de los siguientes comandos:

- **verify-data.sh -v ro [-a repair]**
- **verify-data.bat -v ro [-a repair]**

Verificación de la correlación de herencias

La verificación de la correlación de herencias consulta todas las tablas que correlacionan una clase de elemento de configuración y comprueba que todas las tablas tengan una entrada para cada fila.

Acerca de esta tarea

Cuando se habilita la opción de reparación, los registros se vuelven a crear.

Procedimiento

Para verificar la correlación de herencias, ejecute los siguiente comandos:

- **verify-data.sh -v io [-a repair]**
- **verify-data.bat -v io [-a repair]**

Verificación de duplicados

La verificación de duplicados busca elementos de configuración duplicados en función de los valores de campo de regla de denominación de la base de datos.

Acerca de esta tarea

Con la opción de reparación habilitada, los objetos duplicados se fusionan. Tras la fusión, el objeto permanente se conserva en la base de datos y el objeto transitorio se suprime.

La fusión se realiza mediante varias hebras en paralelo. El número predeterminado de hebras es 5. El número de hebras se puede cambiar en el archivo `collation.properties` mediante la definición del distintivo **com.ibm.cdb.topomgr.dataverification.generator.threadcount** a un número adecuado, como en el ejemplo siguiente:

- **com.ibm.cdb.topomgr.dataverification.generator.ThreadCount=10**

Debe reiniciar el servidor de TADDM después de modificar el número de hebras.

Se pueden producir algunos errores durante la fusión de los objetos. La causa de los errores se incluye en un archivo de registro.

- `ERROR_INVALID_DURABLE_GUID`
- `ERROR_INVALID_TRANSIENT_GUID`

La causa de los errores es que faltan alias en la tabla de alias o que hay un objeto no válido. Debe esperar a que los agentes de limpieza supriman los objetos no válidos.

Procedimiento

Para verificar si hay duplicados, ejecute una de las siguientes opciones:

- **verify-data.sh -v dup [-a repair]**
- **verify-data.bat -v dup [-a repair]**

Verificación de las sobrefusiones

La verificación de las sobrefusiones utiliza los datos recopilados de la tabla ALIASES_JN para encontrar y notificar GUID con un gran número de cambios en los alias maestros.

Acerca de esta tarea

La tabla ALIASES_JN incluye el historial de los cambios en la tabla ALIASES. La sobrefusión es una situación en la que un número pequeño de objetos cambian su padre al mismo objeto de modelo. Los objetos hijo se agrupan alrededor de un cierto número de objetos padre. Las sobrefusiones producidas con anterioridad a la instalación de TADDDM 7.2.1 fixpack 3 no se pueden encontrar porque no hay ningún dato obligatorio en la tabla ALIASES_JN. La verificación no tiene la opción de reparación porque podría encontrar resultados de positivos falsos de informes.

De forma predeterminada, el rastreo detallado se habilita para las clases ComputerSystem, AppServer y Operating System, y todas las clases restantes heredadas de ellas. Si quiere habilitar el rastreo para distintas clases, puede editar la propiedad siguiente en el archivo `collation.properties`:

```
com.ibm.tivoli.namereconciliation.service.overmergeClasses
```

A continuación, se muestra un ejemplo de la propiedad especificada para buscar las clases ComputerSystem, AppServer y Operating System:

```
com.ibm.tivoli.namereconciliation.service.overmergeClasses=
ComputerSystem,AppServer,OperatingSystem
```

Significado de las acciones utilizadas para ejecutar el mandato:

- s1s2s1: la verificación busca elementos de configuración que cambian sus valores de atributo de nombre en bucle. Por ejemplo, se detectaría un sistema informático con la firma A, seguida de la firma B, y luego la firma A nuevamente.
- s1s2s3: la verificación busca elementos de configuración que contienen varios cambios para los atributos de nombre dados.
- m1m2m1: la verificación busca elementos de configuración cuyos GUID han cambiado de GUID maestro muchas veces. Por ejemplo, se detectaría un alias A con un GUID maestro B, más tarde reasignado al GUID maestro C, y luego al GUID maestro B nuevamente.
- m1m2m3: la verificación busca elementos de configuración cuyos GUID han cambiado de GUID maestro algunas veces.
- WinCSLinCSWinCS: la verificación busca elementos de configuración que han cambiado de tipo algunas veces. Por ejemplo, se detectaría un sistema informático que se hubiese almacenado en primer lugar como WindowsComputerSystem y luego se hubiese actualizado a LinuxUnitaryComputerSystem, para volver a WindowsComputerSystem.

Procedimiento

Para comprobar las sobrefusiones, ejecute uno de los siguientes comandos:

- **verify-data.sh -v om [-a <action>] [-p <class>] [-from <time stamp>] [-to <time stamp>]**
- **verify-data.bat -v om [-a <action>] [-p <class>] [-from <time stamp>] [-to <time stamp>]**

  donde:

  – **<action>**: s1s2s1, s1s2s3, m1m2m1, m1m2m3, WinCSLinCSWinCS
  – **<class>**: cualquier clase del modelo de TADDM, como ComputerSystem.
  – **<time stamp>**: indicación de fecha y hora con el formato AAAA-MM-DD HH24:MI:SI.

Ejemplo

```
verify-data.sh -v om -a s1s2s1 m1m2m1 WinCSLinCSWinCS
-p ComputerSystem -from 2012-11-13 14:50:00 -to 2012-11-14 14:50:01
```

Este mandato busca sobrefusiones de tipo s1s2s1, m1m2m1 y WinCSLinCSWinCS para la clase ComputerSystem, y todas las clases que heredan de ella, creada entre el 2012-11-13 14:50:00 y el 2012-11-14 14:50:01.

Solución del problema de la sobrefusión:

La sobrefusión se produce cuando un número pequeño de objetos cambian su padre al mismo objeto de modelo. Los objetos hijo se agrupan alrededor de un cierto número de objetos padre.

Procedimiento

1. Ejecute la verificación de sobrefusiones.
2. Compruebe los elementos de configuración notificados. La verificación podría notificarlos de forma incorrecta como sobrefusiones.
3. Corrija la configuración en entornos que podrían ser la causa de la sobrefusión. Entre los problemas de configuración podrían estar la misma signatura, número de serie, VMID y otros atributos de nombre de los CI.
4. Elimine los objetos sobrefusionados de la base de datos TADDM.
5. Ejecute un descubrimiento en los objetos eliminados y valide los resultados.
6. Elimine todos los registros de la tabla ALIASES_JN después de resolver los problemas de sobrefusión.

Gestión de la memoria caché de credenciales - programa de utilidad cachemgr

Puede utilizar el mandato **cachemgr.sh** o **cachemgr.bat** para listar y suprimir el contenido de la memoria caché de credenciales.

Sintaxis del mandato

cachemgr -h | **-u** *usuario* **-p** *contraseña* (**-l** | **-r**) *valid* | *invalid* | *all* [[**-s** *IP* | *ámbito* | *grupo ámbitos* | *rango* | *subred*] [**-a** *espacioDirecciones*] [**-n** *nombreCredencialAcceso*] [**-c** *tipo*] [**-d** *aaaa/mm/dd*] [**-k** *clave*] [**-t** *etiquetaUbicación*]]

Parámetros

-a, --addressSpace *espacioDirecciones*
Es el nombre del espacio de direcciones.

-c, --class *tipo*
Es el tipo de la entrada de acceso seleccionada que se describe mediante el nombre de la clase específica que implementa la entrada de acceso.

-d, --date *aaaa/mm/dd*
Es el umbral de fecha que se utiliza para seleccionar entradas no modificadas hasta la hora especificada. El formato es aaaa/mm/dd.

-h, --help
Muestra la ayuda.

-k, --key *clave*
Es la clave de una entrada en almacenamiento caché seleccionada.

-l, --list *valid|invalid|all*
Es la operación de listado que se controla mediante los argumentos siguientes:

- *valid* - solo lista los intentos de autenticación válidos que se conservan en la memoria caché.
- *invalid* - solo lista los intentos de autenticación no válidos que se conservan en la memoria caché.
- *all* - lista los intentos de autenticación válidos y no válidos que se conservan en la memoria caché.

-n, --name *nombreCredencialAcceso*
Es el nombre de las credenciales de acceso, el mismo que figura en la lista de acceso.

-p, --password *contraseña*
Es la contraseña del usuario que inicia sesión en el servidor de TADDM.

-r, --remove *valid|invalid|all*
Es la operación de eliminación que se controla mediante los argumentos siguientes:

- *valid* - solo elimina los intentos de autenticación válidos que se conservan en la memoria caché.
- *invalid* - solo elimina los intentos de autenticación no válidos que se conservan en la memoria caché.
- *all* - elimina los intentos de autenticación válidos y no válidos que se conservan en la memoria caché.

-s, --scope *IP|ámbito|grupo de ámbitos|rango|subred*
Es el ámbito de una entrada en almacenamiento caché. Se controla mediante los argumentos siguientes:

- *IP*
- *ámbito*
- *grupo ámbitos*
- *rango*
- *subred*

-t, --locationTag *etiquetaUbicación*
Es la etiqueta de ubicación de una entrada de acceso seleccionada.

-u, --username *nombreusuario*
Es el usuario que inicia la sesión en el servidor TADDM.

Ejemplos

- El siguiente mandato lista todos los intentos de autenticación no válidos para sistemas en el ámbito `"ScopeSet"`:

```
cachemgr.sh -u user -p password -l invalid -s ScopeSet
```

Este mandato genera la salida siguiente:

```
Las siguientes entradas coinciden con los criterios proporcionados:
CachedAuthEntry
 guid: 3B954CE4CFBF346C8DF538F09F1F7FFD
 keyString: SSH!9.128.109.144!!com.collation.platform.security.auth.HostAuth!null!
 lastModified: Thursday, 5 September 2013 11:00:38
 Authorization: invalid. Mensaje de error: CTJTP1190E El servidor no ha podido completar
el proceso de autorización.
CachedAuthEntry
 guid: ACC2F35A66D3379BAC13FC606C5A08A3
 keyString: SSH!9.128.109.145!!com.collation.platform.security.auth.HostAuth!null!
 lastModified: Thursday, 5 September 2013 11:00:38
 Authorization: invalid. Mensaje de error: CTJTP1190E El servidor no ha podido completar
el proceso de autorización
```

- El mandato siguiente suprime los intentos de autenticación en el rango de IP 9.123.149.10 - 9.123.149.12 y la entrada de acceso `com.collation.platform.security.auth.HostAuth`:

```
cachemgr.sh -u user -p password -r invalid -s 9.123.149.10-9.123.149.12
-c com.collation.platform.security.auth.HostAuth
```

Este mandato genera la salida siguiente:

```
AuthEntries eliminadas correctamente de la memoria caché (2).
```

Códigos de retorno del programa de utilidad Cachemgr

Si escribe un script cron o algún otro script que invoca el programa de utilidad cachemgr, los siguientes códigos de retorno indican la salida del programa.

0 El programa se ha completado correctamente.

1 Se ha suministrado un parámetro de línea de mandatos. El parámetro o los datos que se han suministrado con el parámetro son incorrectos. Corrija el mandato y vuelva a intentarlo.

2 Un parámetro de línea de mandatos de fecha no tenía el forma previsto.

3 La definición de ámbito no se resuelve en ninguna dirección IP o la entrada de acceso proporcionada no es válida.

4 Se ha producido un error desconocido. Vaya al directorio de registro y abra `cachemgr.log` para buscar más información.

5 El usuario proporcionado no tiene los privilegios necesarios (descubrimiento) para realizar la operación.

6 No hay entradas en la base de datos que coincidan con el criterio proporcionado.

Preparación del descubrimiento

Para optimizar la información que recopila TADDM desde su entorno durante los descubrimientos, debe completar las tareas de configuración para preparar su entorno para descubrimiento.

Acerca de esta tarea

Las tareas específicas de configuración específicas dependen del tipo y el nivel de descubrimiento al que necesite dar soporte en su entorno.

Qué hacer a continuación

Además de configurar el entorno para el descubrimiento, debe configurar los sensores de TADDM, según sea necesario. Para obtener información sobre cómo hacerlo, consulte la *referencia del sensor* de TADDM.

Para obtener información sobre cómo ejecutar un descubrimiento, incluida la definición de un ámbito y la definición de una planificación, consulte la *Guía del usuario* de TADDM .

Configuración del ID de inicio de sesión de usuario

TADDM requiere un usuario interactivo para poder ejecutar correctamente los descubrimientos. Debe configurar el ID de inicio de sesión de usuario.

Se utiliza un ID de inicio de sesión de usuario interactivo en una modalidad no interactiva para todas las sesiones de descubrimiento, incluida una sesión de servidor a pasarela y una sesión de pasarela a destino. El usuario debe ser interactivo para poder ejecutar mandatos. No obstante, los mandatos se ejecutan de forma no interactiva, lo que significa que un usuario ejecuta el mandato y espera los resultados.

En `/etc/passwd`, establezca el usuario de la siguiente manera:

taddmusr`:x:100:100::/export/home/`*taddmusr*`:/bin/sh`

donde *taddmusr* es el nombre de usuario de TADDM.

Configuración de métodos alternativos de descubrimiento

Es posible que desee utilizar métodos alternativos de descubrimiento como el descubrimiento asíncrono, el descubrimiento basado en scripts o el descubrimiento utilizando IBM Tivoli Monitoring.

Notas:

1. El descubrimiento asíncrono y el descubrimiento basado en scripts solo está soportado si el sistema de destino se ejecuta en el sistema operativo AIX, FreeBSD, HP NonStop, Linux (solo en sistemas x86), Solaris o Windows.
2. Si el sistema de destino ejecuta un sistema operativo Solaris, el descubrimiento basado en script es posible que no funcione si se utiliza SunSSH 1.0.

Configuración del descubrimiento asíncrono

Para ejecutar un descubrimiento asíncrono, primero debe configurar el descubrimiento.

Acerca de esta tarea

Para configurar un descubrimiento asíncrono, debe generar un paquete de script de descubrimiento, copiar el paquete al sistema de destino y ejecutar el script en el sistema de destino. La salida del script de descubrimiento es un archivo de archivado que contiene los resultados del descubrimiento. A continuación, debe mover este archivo de archivado al servidor de TADDM.

Nota: Si ha configurado el descubrimiento se ejecute en modalidad asíncrona y después ha actualizado el TADDM, debe generar de nuevo un paquete de scripts de descubrimiento porque puede cambiar el ID del plug-in del sensor.

Procedimiento

1. Para generar un paquete de script de descubrimiento, introduzca uno de los siguientes mandatos desde el directorio `$COLLATION_HOME/bin`:

   - **Método regular**

     ```
     makeASDScriptPackage DIR_SALIDA NOMBREU
     [DIRECCIÓNIP] [MÉTODO_EMPAQUETADO]
     ```

     DIR_SALIDA
     Vía de acceso del directorio para el paquete de script.

     NOMBREU
     El sistema operativo del sistema de destino en el que se debe ejecutar el script. Los valores válidos son `AIX`, `Linux`, `SunOS`, `FreeBSD`, `Windows` o `NONSTOP_KERNEL`.

     DIRECCIÓNIP **(opcional)**
     Dirección IP del sistema de destino en el que se ejecuta el script.

     Los scripts que se utilizan para el descubrimiento asíncrono utilizan la información de las propiedades del servidor TADDM definidas en el archivo `collation.properties`, y algunas de ellas pueden ser propiedades con ámbito.

     propiedad con ámbito
     Propiedad a la que puede añadir una dirección IP o el nombre de un conjunto de ámbitos. La dirección IP o el nombre del conjunto de ámbitos hacen que la propiedad dependa del host que se está descubriendo. Únicamente puede utilizar nombres de conjuntos de ámbitos que no contengan espacios, apóstrofos ('), puntos (.) y barras inclinadas (/).

     Si ha personalizado cualquiera de las propiedades del servidor de TADDM de modo que tengan ámbito, debe incluir la opción *DIRECCIÓNIP* en el mandato **makeASDScriptPackage**.

     MÉTODO_EMPAQUETADO **(opcional)**
     Método utilizado para empaquetar los archivos. Los valores válidos son `tar` o `zip`.

     Si no se especifica ningún método, éste lo determina el sistema operativo. Por ejemplo, para sistemas operativos, como Linux, se utiliza el método tar.

     De forma predeterminada, la vía de acceso al sistema se busca para el programa de utilidad de archivado. Si es necesario, añada la propiedad `com.ibm.cdb.tarpath` al archivo `collation.properties`, y especifique una vía de acceso alternativa para el programa de utilidad de archivado.

     En los sistemas operativos Solaris, debido a una limitación en la longitud de los nombres de archivos, debe utilizar el programa de utilidad de archivado gtar y debe especificar la vía de acceso al programa de utilidad.

     El ejemplo siguiente muestra cómo especificar la vía de acceso del mandato **tar** en el servidor TADDM para el sistema operativo AIX:

     ```
     com.ibm.cdb.tarpath=tar
     ```

Los ejemplos siguientes muestran cómo especificar la vía de acceso del mandato **tar** *en el sistema de destino*, en función del sistema operativo:

Para AIX

```
com.ibm.cdb.targettarpath.AIX=tar
```

Para Solaris

```
com.ibm.cdb.targettarpath.SunOS=/usr/sfw/bin/gtar
```

Por ejemplo, para generar un paquete de script de descubrimiento para el sistema operativo AIX, especifique el siguiente mandato:

```
./makeASDScriptPackage /tmp AIX
```

Este mandato crea el siguiente paquete de script de AIX en el directorio `tmp`: `/tmp/taddm_AIX.tar`.

- **Método ampliado**

  `makeASDScriptPackage --outputDir` *`OUTPUT_DIR`* `--uname` *`UNAME`*
  `[--ipAddress` *`IP_ADDRESS`*`] [--packingMethod` *`PACKING_METHOD`*`] [--sensors` *`SENSOR`*`]`

  --outputDir *OUTPUT_DIR*
  Consulte la descripción del parámetro *OUTPUT_DIR* del método regular.

  --uname *UNAME*
  Consulte la descripción del parámetro *UNAME* del método regular.

  [--ipAddress *IP_ADDRESS*] (opcional)
  Consulte la descripción del parámetro *IPADDRESS* del método regular.

  [--packingMethod *PACKING_METHOD*] (opcional)
  Consulte la descripción del parámetro *PACKING_METHOD* del método regular.

  [--sensors *SENSOR*] (opcional)
  El nombre del sensor que desea incluir en el paquete. La siguiente tabla contiene los nombres de sensores que se deben utilizar en este mandato.

Tabla 33. Nombres de sensores utilizados en el mandato **makeASDScriptPackage**.

Sensor	Nombre utilizado en el mandato
Sensor de Apache	apacheserver
Sensor de Citrix XenServer	xenserver
Sensor de sistemas FreeBSD	computersystem
Sensor de servidor genérico	genericserver
Sensor del sistema HP NonStop	computersystem
Sensor del sistema IBM AIX	computersystem
Sensor de IBM DB2	db2
Sensor de servidor IBM Lotus Domino	dominoserverinitial
Sensor de IBM Tivoli Utilization	utilization
Sensor de IBM WebSphere MQ Server	mqserver
Sensor de IBM WebSphere	webspherescript
Sensor de JBoss Application Server 7	jboss7
Sensor de KVM	kvm

Tabla 33. Nombres de sensores utilizados en el mandato **makeASDScriptPackage**. *(continuación)*

Sensor	Nombre utilizado en el mandato
Sensor de sistema Linux	computersystem
Sensor de Microsoft Exchange	exchange
Sensor del servidor web Microsoft IIS	iisserver
Sensor de Oracle	oracle
Sensor de sistema Solaris	computersystem
Sensor SSH de WebLogic	weblogiclaunchersensor
Sensor de sistema Windows	computersystem

El sensor de descubrimiento asíncrono se añade de forma predeterminada a todos los paquetes. Todos los sensores de sistema operativo tienen el nombre `computersystem`. Se diferencian a partir del parámetro `--uname`. Por ejemplo, si especifica los siguientes parámetros:

```
[...] --uname Linux --sensors computersystem
```

Se añadirá el sensor de sistema Linux al paquete.

Por ejemplo, para generar un paquete de script de descubrimiento para el sistema operativo AIX, especifique el siguiente mandato:

```
./makeASDScriptPackage --outputDir /tmp --uname AIX --sensors computersystem
```

Este mandato crea el siguiente paquete de script de AIX en el directorio `tmp`: `/tmp/taddm_AIX.tar`.

2. Copie el paquete de script de *DIR_SALIDA* al sistema de destino y extraiga el paquete de script.
3. Como usuario root en sistemas UNIX, o como administrador en el sistema Windows, otorgue privilegios de ejecución a todos los archivos de script. Si el script de descubrimiento se ejecuta como un usuario no root, o como un usuario no administrador, es posible que algunos scripts de sensor no completen un descubrimiento correcto, o que los datos que descubre el sensor sean limitados.
4. Ejecute el script **scriptsRunner.sh** para los destinos UNIX, o **scriptsRunner.bat** para el destino Windows.
5. Mueva el archivo de archivado resultante (por ejemplo, `/tmp/taddm${`*`versión`*`}/asd/taddmasd-${`*`nombre_host`*`}-${`*`indicación_fecha_hora_ejecución`*`}.tar`) al servidor TADDM de la ubicación definida por la propiedad `com.ibm.cdb.discover.asd.AsyncDiscoveryResultsDirectory` al archivo `collation.properties`.
6. En el archivo `collation.properties`, defina el valor de la propiedad `com.ibm.cdb.discover.asd.ProcessUnreachableIPs` en `true`.
7. Asegúrese de que el sensor de descubrimiento asíncrono (`ASDSensor`) está habilitado en el perfil de descubrimiento. De forma predeterminada, el sensor está habilitado en los perfiles de descubrimiento de nivel 2 y nivel 3.
8. Cree el ámbito con la dirección IP del sistema de destino.

Qué hacer a continuación

Ejecute el descubrimiento. No necesita una autorización de usuario root para ejecutar este descubrimiento.

Durante el descubrimiento, si el ping, el puerto o el sensor de la sesión no pueden acceder al sistema operativo, el sistema de destino se considera inalcanzable. Si el valor de la propiedad `com.ibm.cdb.discover.asd.ProcessUnreachableIPs` se define en `true`, el sensor de descubrimiento asíncrono se ejecuta para procesar el archivo de archivado para el sistema de destino. El archivo de archivado se procesa sólo si la dirección IP del ámbito de descubrimiento coincide con la dirección IP del sistema que produjo el archivo de archivado. Según el contenido del archivo de archivado, los sensores de planificarán para procesar la salida del script. Después de haberse procesado el archivo de archivado. se renombra como *NombreArchivoCinta*`.tar_DONE` por lo que no se vuelve a procesar.

El archivo de archivado de descubrimiento sólo se procesa una vez. Si el sensor no está habilitado para procesar la salida de script en el momento del procesamiento del archivo de archivado, la ejecución de un segundo descubrimiento con el sensor habilitado no procesa un archivo de archivado previamente procesado, excepto que se completen los siguientes pasos:

1. Renombre el archivo de archivado a su nombre original. Por ejemplo, elimine `_DONE` del nombre del archivo.
2. El archivo `.processed` del directorio `$COLLATION_HOME/var/asdd` contiene una lista de archivos de archivado procesados. Elimine el nombre del archivo de archivado del archivo `.processed`.

Se pueden procesar diferentes archivos de archivado procedentes de diversos sistemas en una única ejecución de descubrimiento, pero sólo se procesa un archivo de archivado por sistema de destino durante una única ejecución de descubrimiento. Si un sistema de destino tiene varios archivos de archivado, sólo se procesa el único con la indicación de fecha y hora más recientes.

Para descubrir diferentes archivos de archivado procedentes de diversos sistemas en una única ejecución de descubrimiento, copie cada archivo de archivado en una ubicación que esté definida por la propiedad `com.ibm.cdb.discover.asd.AsyncDiscoveryResultsDirectory`. Incluya la dirección IP de cada sistema de destino en el ámbito de descubrimiento.

Como el script de descubrimiento utiliza el mandato **`tar`** para crear el archivo de archivado del descubrimiento, si utiliza el servidor de TADDM que está en ejecución en el sistema operativo Windows, debe instalar un programa de cinta de terceros para que TADDM lo utilice para extraer los archivos del archivo de archivado. La ubicación del programa de cinta está definida por la propiedad `com.ibm.cdb.tarpath`.

Restricción: El programa tar debe admitir rutas de archivo largas. GNU Tar 1.13 no se admite porque podría truncar nombres de archivo largos.

Configuración del descubrimiento basado en script

Para ejecutar un descubrimiento basado en script, primero debe configurar el descubrimiento.

Acerca de esta tarea

En comparación con los sensores normales, los sensores ejecutados en la modalidad basada en scripts son más aparentes, lo que significa que todos los mandatos que utiliza el sensor están en un script, que puede ver. Para obtener la lista de los sensores que soportan la modalidad basada en scripts, y las restricciones que se aplican a algunos de los sensores, consulte el tema *Sensores que*

soportan el descubrimiento asíncrono y basado en scripts de la *Referencia de sensores* de TADDM.

Procedimiento

Configure el sensor de una de las siguientes maneras:

- **Habilitación de todos los sensores que soportan el descubrimiento basado en scripts** Para habilitar globalmente todos los sensores que soportan un descubrimiento basado en scripts, abra el archivo `collation.properties` y defina el valor de la propiedad `com.ibm.cdb.discover.PreferScriptDiscovery` en `true`.

- **Habilitación de todos los sensores que soportan el descubrimiento basado en scripts en un perfil de descubrimiento específico**
  Para habilitar todos los sensores que soportan un descubrimiento basado en script para un perfil de descubrimiento específico, complete los pasos siguientes:
  1. En el Portal de gestión de descubrimiento, seleccione el perfil de descubrimiento para el que desea habilitar la modalidad basada en scripts.
  2. En el separador **Propiedades de plataforma**, defina el valor de la propiedad `com.ibm.cdb.discover.PreferScriptDiscovery` en `true`.

- **Habilitación de un sensor que soporta el descubrimiento basado en scripts en un archivo de descubrimiento**
  Para habilitar un sensor específico que soporta un descubrimiento basado en script en un perfil de descubrimiento, actualice la configuración del sensor en el perfil de descubrimiento correspondiente. Efectúe los pasos siguientes:
  1. En el Portal de gestión de descubrimiento, vaya al perfil de descubrimiento que contiene el sensor que desea habilitar.
  2. En el separador **Configuración de sensor**, seleccione el sensor y pulse **Nuevo**.
  3. En la ventana Crear configuración, especifique el nombre de la configuración y seleccione la opción **Descubrimiento basado en el script Perform**.
  4. Pulse **Aceptar** para guardar la configuración.

Qué hacer a continuación

Configuración de TADDM para seleccionar usuarios no predeterminados para el descubrimiento

De forma predeterminada, solo se utiliza el usuario solicitado por el script para el descubrimiento. Si encuentra problemas al ejecutar un descubrimiento con el usuario predeterminado y tiene otro usuario que tenga todos los permisos necesarios, puede configurar TADDM para seleccionar este usuario para el descubrimiento.

Nota: Utilice la configuración siguiente con cuidado. Si se utiliza para un descubrimiento un usuario que no tenga todos los permisos necesarios, el descubrimiento podría fallar, o es posible que algunos de los destinos no se descubran.

En el archivo `plugin.xml` que puede encontrar en un paquete para cada sensor del directorio `COLLATION_HOME/osgi/plugins`, edite la definición de nodos `script`, por ejemplo, como en el fragmento `plugin.xml` del sensor de IBM WebSphere MQ Server:

```
<scriptset>
   <ostype>AIX</ostype>
   <mainScript name="sensorCommon.sh" />
   <script name="script.sh" authClassName="com.collation.platform.security.
auth.MQServerAuth" authMode="preferred" hostAuthFallback="true"/>
</scriptset>
```

Pueden definirse las siguientes propiedades:

authMode
Define cómo enfoca TADDM las entradas de la lista de acceso para el tipo especificado por `authClassName`. Están disponibles los siguientes valores:

- `single`: sólo se utiliza un usuario solicitado por el script. Éste es el valor predeterminado.
- `preferred`: en primer lugar, se utiliza un usuario preferido por el script, pero si no está disponible o falla, se utilizan las restantes entradas de la lista de acceso del tipo definido.
- `regular`: se utilizan las entradas de la lista de acceso en el orden especificado sin comprobar las preferencias del usuario.

hostAuthFallback
Define si hay problemas para establecer la conexión con el destino para un `authClassName` específico o el usuario preferido, o ambos, si TADDM vuelve a la sesión establecida por el usuario genérico que se utiliza para conectarse al destino. Están disponibles los siguientes valores:

- `false`: el valor predeterminado.
- `true`.

Configuración del descubrimiento mediante IBM Tivoli Monitoring (método antiguo)

TADDM puede realizar descubrimientos de nivel 1, nivel 2 y algunos de nivel 3 mediante la infraestructura deIBM Tivoli Monitoring 6.2.1 o posterior.

Método de integración antiguo
Esta sección está dedicada a un método en desuso de la integración de TADDM con IBM Tivoli Monitoring. A partir de la versión 7.3.0 de TADDM se recomienda efectuar la integración con IBM Tivoli Monitoring 6.3 mediante la automatización de OSLC. El método antiguo de la integración con el uso del sensor de IBM Tivoli Monitoring Scope está en desuso y se eliminará en los próximos releases. Para obtener más información sobre la configuración del descubrimiento mediante la automatización de OSLC, consulte “Configuración del descubrimiento mediante la sesión de automatización de OSLC” en la página 116.

Si utiliza IBM Tivoli Monitoring 6.2.1-TIV-ITM-FP0001, 6.2.2-TIV-ITM-FP0002, o un nivel posterior, puede descubrir los puntos finales de Tivoli Monitoring a través de Tivoli Enterprise Portal Server. Estos fixpacks resuelven el APAR IZ63983, lo que mejora el rendimiento de Tivoli Monitoring durante los descubrimientos de TADDM. El uso de versiones o niveles anteriores de IBM Tivoli Monitoring para

realizar descubrimientos de TADDM a través de Tivoli Enterprise Portal Server podría causar una carga excesiva del procesador o la red, especialmente en componentes de Tivoli Monitoring.

Nota: El descubrimiento mediante IBM Tivoli Monitoring solo es posible cuando la base de datos Tivoli Enterprise Portal Server está en Microsoft SQL Server y DB2. No es posible cuando se utiliza la base de datos Apache Derby como la base de datos de Tivoli Enterprise Portal Server.

Propiedades del servidor TADDM específicas del descubrimiento mediante Tivoli Monitoring

Para obtener información acerca de las propiedades del servidor TADDM que son específicas del descubrimiento mediante IBM Tivoli Monitoring, incluidas las propiedades que afectan al modo en que TADDM descubre los puntos finales de Tivoli Monitoring, consulte "Propiedades del descubrimiento mediante IBM Tivoli Monitoring (método antiguo)" en la página 84.

En un perfil de descubrimiento, puede configurar las propiedades del servidor TADDM que afectan al modo en que TADDM descubre los puntos finales de Tivoli Monitoring. Para ello, realice los pasos siguientes, en función de si utiliza un perfil personalizado o el perfil predeterminado:

Configuración de las propiedades para un perfil personalizado

1. Inicie la consola de Discovery Management.
2. Abra **Perfiles de descubrimiento**.
3. Pulse el perfil de descubrimiento que desee configurar.
4. Pulse el separador **Propiedades de plataforma**.
5. Cambie el valor de la propiedad que desea actualizar y seleccione el recuadro de selección **Incluido** para esta propiedad.
6. Guarde los cambios.

Configuración de las propiedades para el perfil predeterminado.

En el archivo `$COLLATION_HOME/etc/collation.properties`, añada (o edite) la propiedad respectiva, como se indica en el siguiente ejemplo, donde *perfil_descubrimiento* representa el nombre de perfil:

```
com.ibm.cdb.session.allow.ITM.perfil_descubrimiento=true
```

Por ejemplo, la propiedad siguiente especifica que TADDM utiliza el perfil de descubrimiento "Descubrimiento de utilización" y utiliza IBM Tivoli Monitoring para descubrir los puntos finales de Tivoli Monitoring:

```
com.ibm.cdb.session.allow.ITM.Utilization_Discovery=true
```

Nota: En el archivo `collation.properties`, debe sustituir el carácter de espacio entre "Utilization" y "Discovery" del nombre de perfil por un carácter de guión bajo.

Propiedades del servidor TADDM adicionales que es posible que necesite configurar

Las siguientes sugerencias de configuración describen propiedades adicionales del servidor TADDM que es posible que necesite configurar:

- El valor de la propiedad siguiente, que es específica de los sistemas Windows, se debe establecer en `true` (el valor predeterminado) para habilitar el descubrimiento de los sistemas Windows de destino en el descubrimiento

mediante IBM Tivoli Monitoring. Si se establece el valor en `false`, TADDM no puede establecer una sesión IBM Tivoli Monitoring con los sistemas de destino Windows.

```
com.collation.AllowPrivateGateways=true
```

- Se puede producir un alto uso del procesador en Tivoli Enterprise Portal Server durante el descubrimiento. Para minimizar esto, puede limitar el número de hebras Worker del descubrimiento que se ejecutan durante el descubrimiento. En el servidor de TADDM, defina la siguiente propiedad del servidor:

  ```
  com.collation.discover.dwcount=16
  ```

- En un amplio entorno de IBM Tivoli Monitoring, el sensor de IBM Tivoli Monitoring Scope podría detenerse con un tiempo de espera antes de finalizar. Para permitir un mayor tiempo de procesamiento, defina las siguientes propiedades del servidor:

  ```
  com.collation.platform.session.ITMSessionNumProgressChecks=3600
  com.collation.discover.agent.ITMScopeSensor.timeout=3600000
  ```

Configuración del descubrimiento mediante la sesión de automatización de OSLC

TADDM puede ejecutar el descubrimiento de nivel 2 y algunos descubrimientos de nivel 3 utilizando OSLC.

Antes de empezar

Para configurar el descubrimiento en los conjuntos de ámbitos proporcionados por los proveedores de servicios de automatización de ejecución de OSLC, debe cumplir los siguientes requisitos:

- Debe tener al menos un proveedor de servicios de automatización de ejecución de OSLC instalado y operativo.
- TADDM debe estar conectado al proveedor de servicios de automatización de ejecución de OSLC.

Procedimiento

Para ejecutar un descubrimiento mediante una sesión de automatización de OSLC, siga estos pasos:

1. Añada las credenciales de acceso del producto que desee integrar con la lista de acceso. Para ello, cree una nueva entrada de lista de acceso del tipo `"Integration">"OSLC Automation"`. Si desea integrar TADDM con ITM, proporcione las credenciales de ITM TEPS. Durante el descubrimiento, se utilizan las entradas de lista de acceso de automatización de OSLC y el tipo de entrada de lista de acceso de ITM para garantizar la compatibilidad con las versiones anteriores.
2. Compruebe el ámbito de descubrimiento. OSLCAutomationAgent crea de forma periódica los conjuntos de ámbitos. Los nuevos conjuntos de ámbitos se muestran en el separador **Conjuntos de ámbitos**. Si desea integrar TADDM con ITM, se crea un conjunto de ámbitos para cada ITM TEMS. Puede ejecutar OSLCAutomationAgent manualmente utilizando el siguiente mandato:

   ```
   /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent
   ```

3. Configure las propiedades de descubrimiento que permiten utilizar la sesión de automatización de OSLC. Puede establecer las propiedades en el archivo `collation.properties` o en un nuevo perfil de descubrimiento personalizado.
   - El archivo `collation.properties`:

     ```
     com.ibm.cdb.session.prefer.OSLCAutomation=true
     com.ibm.cdb.session.allow.OSLCAutomation=true
     ```

Los ejemplos de propiedades con ámbito:

```
com.ibm.cdb.session.prefer.OSLCAutomation.9.222.222.124=false
com.ibm.cdb.session.prefer.OSLCAutomation.Level_3_Discovery=false
```

- Perfil de descubrimiento personalizado. En la consola de Discovery Management, cree un nuevo perfil de descubrimiento y configure el separador **Propiedades de plataforma** de la siguiente manera:

```
com.ibm.cdb.session.allow.OSLCAutomation=true
com.ibm.cdb.session.prefer.OSLCAutomation=true
```

4. Ejecute un descubrimiento normal de los ámbitos creados por OSLCAutomationAgent eligiendo uno de los métodos siguientes:
   - El perfil L2 o L3 predeterminado cuando el archivo `collation.properties` se ha configurado para dar soporte a la sesión de automatización de OSLC.
   - El nuevo perfil de descubrimiento con el separador **Propiedades de plataforma** configurado correctamente.

Referencia relacionada:

"Propiedades para el descubrimiento utilizando la sesión de automatización de OSLC" en la página 86
Estas propiedades se aplican al descubrimiento utilizando la sesión de automatización de OSLC.

"Interfaz de línea de mandatos para OSLCAutomationAgent" en la página 215
OSLCAutomationAgent se utiliza para recopilar datos de los proveedores de servicios de automatización de ejecución de OSLC. Puede utilizar mandatos para ejecutar el agente manualmente y para renovar o actualizar los conjuntos de ámbitos que crea.

Configuración del nivel de descubrimiento

Debe configurar el nivel de descubrimiento.

Configuración del descubrimiento de nivel 1

Se necesita una configuración mínima para el descubrimiento de nivel 1 (descubrimiento sin credenciales), que explora la pila TCP/IP para recopilar información básica sobre los sistemas informáticos activos.

Acerca de esta tarea

Para el descubrimiento de nivel 1, configure los dispositivos de red del entorno que desee que el servidor de TADDM descubra.

Procedimiento

Para ello, realice los pasos siguientes:

1. En función de la versión de SNMP de que disponga, grabe la información siguiente para utilizarla con el servidor de TADDM:
   - Para SNMP V1 y V2, registre la serie SNMP MIB2 GET COMMUNITY.
   - Para SNMP V3, registre el nombre de usuario y la contraseña de SNMP.
2. Asigne permiso a MIB2 System, IP, Interfaces e Interfaces ampliadas.

Configuración del descubrimiento de nivel 2

Además de los requisitos necesarios para el descubrimiento de nivel 1, el descubrimiento de nivel 2 necesita que se lleven a cabo ciertas tareas de configuración adicionales para poder dar soporte al descubrimiento de información detallada de configuración de hosts.

Antes de empezar

Si los sistemas de destino son puntos finales de IBM Tivoli Monitoring descubiertos por el sensor IBM Tivoli Monitoring Scope, las credenciales para esos sistemas de destino no son necesarias para el descubrimiento de nivel 2. Para obtener más información, consulte las siguientes fuentes:

- "Integración de TADDM con IBM Tivoli Monitoring (método antiguo)" en la página 216
- "Configuración del descubrimiento mediante IBM Tivoli Monitoring (método antiguo)" en la página 114
- TADDM *Sensor Reference* para obtener información acerca del sensor de IBM Tivoli Monitoring Scope

Acerca de esta tarea

En los sistemas operativos de destino, en los que desea que TADDM ejecute el descubrimiento, debe configurar como mínimo el software siguiente:

Secure Shell (SSH)
Puede utilizar OpenSSH o la versión que suministra el proveedor de SSH que se proporciona con el sistema operativo. Para obtener más información sobre los sistemas operativos Windows, consulte "Dependencia de Windows Management Instrumentation (WMI)" en la página 132.

SUNWscpu (solo para entornos Solaris)
Para proporcionar información completa sobre procesos, instale el paquete SUNWscpu (Source Compatibility).

Archivos LiSt Open (lsof)
Para proporcionar información completa sobre dependencias, instale el programa LiSt Open Files (lsof) en todos los sistemas informáticos de destino de acuerdo con los requisitos de la sección *Requisitos de lsof* de la Wiki de TADDM en https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/TADDM%20lsof%20requirements.

Creación de la cuenta de servicio:

Debe crear una cuenta de servicio en todos los sistemas informáticos que están descubiertos utilizando conexiones basadas en claves SSH y basadas en contraseñas. Éste es el método primario para descubrir los sistemas informáticos (servidores) en la red.

Acerca de esta tarea

Para simplificar la configuración de descubrimiento, cree la misma cuenta de servicio en cada sistema informático que desea descubrir. La cuenta de servicio debe permitir el acceso a todos los recursos del sistema informático de destino que TADDM necesita descubrir. La cuenta de servicio debe tener privilegios de acceso de escritura al directorio de inicio en cada sistema informático de destino. Este directorio requiere aproximadamente 20 MB de espacio libre. Durante un descubrimiento, se pueden almacenar scripts y archivos temporales en este directorio. Después de llevar a cabo un descubrimiento, se suprimen los archivos.

Se puede utilizar una cuenta de servicio con privilegio que no sea raíz. Sin embargo, para que se puedan ejecutar en el sistema de destino, algunos mandatos del sistema operativo que se utilizan durante el descubrimiento pueden requerir

un privilegio superior, como autoridad root (o superusuario).

Procedimiento

Para crear un cuenta de servicio en el sistema de destino realice uno de los procedimientos siguientes:

1. Para un sistema operativo Linux, Solaris, AIX, y Linux para System z, suponga que el nombre de la cuenta de servicio es `coll` y utilice los mandatos siguientes para crear la cuenta de servicio:

   ```
   # mkdir -p /export/home/coll
   # useradd -d /export/home/coll -s /bin/sh \
      -c "Service Account" -m coll
   # chown -R coll /export/home/coll
   ```

2. Para un sistema informático Windows, cree una cuenta de servicio que sea miembro del grupo del administrador local. Esta cuenta puede ser local o de dominio. Dado que TADDM se basa en WMI para el descubrimiento, la cuenta debe tener acceso a todos los objetos WMI en el sistema local. La cuenta de servicio debe crearse en la pasarela de Windows y en todos los sistemas Windows de destino.

   Nota: La cuenta de servicio debe tener acceso de lectura/escritura al directorio `\WINDOWS\system32` o `\WINDOWS\system64` y a los subdirectorios. En los sistemas Windows Server 2008, los nuevos usuarios no tienen el acceso necesario de forma predeterminada, de modo que debe otorgarse explícitamente para la cuenta de servicio.

Configuración del descubrimiento mediante Secure Shell (SSH):

El servidor de TADDM se puede conectar a OpenSSH (versión 1 ó 2) o a la versión de SSH que suministra el proveedor y que se entrega con el sistema operativo.

El servidor de TADDM da soporte a los métodos de autenticación siguientes:

- Inicio de sesión de SSH2 basado en claves (clave RSA o DSA) e inicio de sesión de SSH1 basado en claves (solo RSA)
- Nombre de usuario y contraseña utilizando SSH2, así como nombre de usuario y contraseña utilizando SSH1

Aunque pueda utilizar cualquiera de los métodos de autenticación, es preferible el inicio de sesión SSH2 basado en claves. El servidor prueba automáticamente cada método en el orden indicado anteriormente y utiliza el primer método que funciona correctamente. El servidor de TADDM utiliza entonces el mismo método con el host en toda la ejecución del descubrimiento.

Nota: Para el inicio de sesión SSH2 basado en claves, el servidor de TADDM intenta iniciar la sesión solo con una clave, RSA o DSA, la que encuentre en el servidor de TADDM. Si existen las dos, solo se utiliza RSA.

Creación de pares de claves para el inicio de sesión basado en claves con el servidor TADDM:

Puede crear un par de claves públicas o privadas utilizando el protocolo SSH (Secure Shell) para el inicio de sesión basado en claves con el servidor de TADDM.

Acerca de esta tarea

Dependiendo de la versión de SSH que utilice, el inicio de sesión de SSH basada en claves utiliza las claves que se muestran en la Tabla 34:

Tabla 34. claves de SSH

Versión/algoritmo de SSH	Clave privada	Clave pública
Openssh/SSH2/RSA	$HOME/.ssh/id_rsa	$HOME/.ssh/id_rsa.pub
Openssh/SSH2/DSA	$HOME/.ssh/id_dsa	$HOME/.ssh/id_dsa.pub
Openssh/SSH1/RSA	$HOME/.ssh/identity	$HOME/.ssh/identity.pub
Commercial/SSH2/RSA	$HOME/.ssh2/id_dss_1024_a	$HOME/.ssh2/id_dss_1024_a .pub

También puede generar un par de claves públicas/privadas utilizando OpenSSH, versión 2. Para generar un par de claves públicas/privadas utilizando un programa SSH que no sea OpenSSH u otra versión de OpenSSH, consulte la documentación de SSH.

Procedimiento

Para generar un par de claves públicas/privadas utilizando OpenSSH, versión 2, efectúe los pasos siguientes:

1. Inicie sesión como propietario del servidor de TADDM.
2. Para generar la clave SSH, especifique el mandato siguiente:

   ```
   $ ssh-keygen -t rsa
   ```

   Acepte los valores predeterminados del mandato. TADDM da soporte a pares de claves con o sin frase de contraseña.
3. En cada sistema informático de destino en el que desea permitir un inicio de sesión basado en claves, inserte los contenidos del archivo `id_rsa.pub` en el archivo `$HOME/.ssh/authorized_keys` para la cuenta de servicio. Algunas implementaciones de SSH2 generan las claves en un directorio distinto de `$HOME/.ssh`. Si la implementación SSH genera las claves en un directorio diferente o con otro nombre, copie, enlace o mueva el archivo de claves privadas en el directorio `$HOME/.ssh/id_rsa` o `$HOME/.ssh/id_dsa`, dependiendo del algoritmo.

Adición de una entrada de lista de acceso para la cuenta de servicio del sistema informático:

Para configurar la autenticación de contraseña con Secure Shell (SSH), debe añadir una entrada de lista de acceso para la cuenta de servicio del sistema informático que creó en el sistema de destino.

Para añadir una entrada de lista de acceso para la cuenta de servicio del sistema informático, complete los pasos siguientes:

1. En la página de inicio de TADDM, asegúrese de que se han iniciado todos los servicios de la Consola de administrador.
2. Inicie la consola de Discovery Management.
3. Seleccione el recuadro de selección **Establecer una sesión segura (SSL)** para que pueda utilizar la opción de seguridad SSL. Esta opción cifra todos los

datos, que incluyen nombres de usuario y contraseñas de la lista de acceso, antes de que se transmitan los datos entre la consola de Discovery Management y el servidor de TADDM.

4. Añada una entrada de lista de acceso al sistema informático para la cuenta de servicio y especifique el nombre de inicio de sesión y la contraseña.

Configuración de System p y System i:

El descubrimiento de un sistema basado en la tecnología IBM Power5 (System p o System i) y sus particiones lógicas se efectúa a través de una consola de Discovery Management. TADDM soporta dos tipos de consolas de gestión de descubrimiento: la consola de gestión de hardware (HMC) e Integrated Virtualization Manager (IVM).

TADDM descubre la consola de gestión utilizando SSH. El ámbito de descubrimiento debe incluir la dirección IP de la consola de gestión y la lista de acceso debe incluir una entrada de tipo Sistema informático con las credenciales adecuadas (nombre de usuario y contraseña) especificadas.

Además de las credenciales de usuario, el usuario de descubrimiento debe definirse en la consola de gestión con los permisos mínimos siguientes:

- Consola de gestión de hardware (HMC)
  - Para una consola de gestión HMC, es preciso un usuario basado en el rol **hmcoperator**. Por ejemplo, cree un rol nuevo denominado *taddmViewOnly* basado en el rol hmcoperator. Además, deben asignarse las siguientes tareas de líneas de mandatos al nuevo rol:

    Sistema gestionado
    Necesario para utilizar los mandatos **lshwres** y **lssyscfg**.

    Partición lógica
    Necesaria para utilizar los mandatos **lshwres**, **lssyscfg** y **viosvrcmd**.

    Configuración HMC
    Necesaria para utilizar el mandato **lshmc**.
- Gestor de virtualización integrado (IVM).

  Para una consola de gestión IVM, se necesita un usuario con el rol **Sólo ver**.

Configuración del descubrimiento de nivel 3

Además de los requisitos necesarios para el descubrimiento de nivel 2, el descubrimiento de nivel 3 necesita que se lleven a cabo ciertas tareas de configuración adicionales para poder dar soporte al descubrimiento de datos de configuración de aplicaciones y de hosts.

Configuración de servidores web y de aplicaciones para el descubrimiento:

Debe configurar los servidores web y los servidores de aplicaciones en el entorno que desea que el servidor de TADDM descubra.

En este apartado se proporcionan los pasos necesarios para configurar servidores web y de aplicaciones.

El servidor de Microsoft IIS no requiere configuración. No hay requisitos de acceso especiales. La cuenta de usuario que ya está establecida en el host es suficiente.

Para el servidor web Apache, la cuenta de servicio de TADDM para el sistema host debe tener permisos de lectura para los archivos de configuración, como el archivo `httpd.conf`.

En el caso del servidor web de Oracle iPlanet, la cuenta de servicio de TADDM para el sistema host debe tener permisos de lectura para los archivos de configuración de iPlanet.

Para servidores de Lotus Domino, asegúrese de cumplir los requisitos previos del tema *Sensor de servidor de IBM Lotus Domino* en la *Referencia de sensores* de TADDM.

Configuración de un servidor de aplicaciones Oracle:

El descubrimiento de un servidor de aplicaciones Oracle utiliza archivos JAR que están incluidos en el servidor de aplicaciones Oracle. Estos archivos JAR no se incluyen en la instalación del servidor de TADDM.

Acerca de esta tarea

Existe una propiedad en el archivo `$COLLATION_HOME/etc/collation.properties` para señalar a una instalación existente del servidor de aplicaciones Oracle. El siguiente testo aparece en el archivo`$COLLATION_HOME/etc/collation.properties`:

```
# Location of the root directory for Oracle Application Server on
the Tivoli Application Dependency Discovery Manager
server
# 1. An example is /home/oracle/product/10.1.3/OracleAS_1
# 2. A relative directory is relative to com.collation.home
# 3. This directory (and its subdirectories) must be accessible
     for the user under which the server runs, usually the collation user.
# 4. Ignore if you do not intend to discover an Oracle Application server.
```

Para señalar a una instalación existente del servidor de aplicaciones Oracle, edite la línea siguiente en el archivo `$COLLATION_HOME /etc/collation.properties`:

```
com.collation.oracleapp.root.dir=lib/oracleapp
```

En la instalación de un servidor de aplicaciones Oracle, los directorios que contienen los archivos JAR necesarios son propiedad del usuario `oracle` con los permisos: `rwx------`. Esto significa que ningún otro usuario excepto el propietario (normalmente, una aplicación Oracle) puede acceder a estos directorios. Si se ejecuta el servidor de TADDM utilizando el usuario `oracle`, estos directorios están accesibles. No obstante, si este no es el caso, debe cambiar los permisos de directorio de los siguientes directorios a `711`, de manera que todos los usuarios puedan acceder a ellos:

- *OracleAppServerHome*
- *OracleAppServerHome*`/j2ee`
- *OracleAppServerHome*`/j2ee/home`
- *OracleAppServerHome*`/opmn`
- *OracleAppServerHome*`/opmn/lib`, donde un ejemplo de *OracleAppServerHome* es `/home/oracle/product/10.1.3/OracleAS_1`

Para descubrir un servidor de aplicaciones Oracle, debe establecer la propiedad com.collation.platform.os.ignoreLoopbackProcesses en el archivo `$COLLATION_HOME/etc/collation.properties` en `true`:

```
com.collation.platform.os.ignoreLoopbackProcesses=true
```

Procedimiento

Para configurar la lista de acceso, efectúe los pasos siguientes:

1. En la consola de Discovery Management, cree una definición de ámbito de descubrimiento que incluya el servidor de la aplicación Oracle o utilice un ámbito existente que contenga el servidor de la aplicación Oracle.
2. Para crear una lista de acceso, pulse el icono **Lista de acceso**.
3. En la ventana Lista de acceso, pulse **Añadir**.
4. En el campo **Tipo de componente** de la ventana Detalles de acceso, pulse **Servidores de la aplicación**.
5. En el campo **Proveedor**, pulse **Servidor de aplicaciones Oracle**.
6. Escriba las credenciales del servidor de la aplicación Oracle.

Configuración del servidor de Microsoft Exchange:

Es preciso que configure el servidor Microsoft Exchange que desea que descubra el servidor TADDM.

Acerca de esta tarea

Para descubrir el Servidor de Microsoft Exchange, el servicio de Microsoft Exchange Management debe ejecutarse en el sistema Windows de destino. El ID de servicio de Windows para la cuenta de servicio de TADDM debe crearse en el sistema Windows en el que se ejecuta el servidor de Microsoft Exchange. El ID de servicio de Windows debe tener permiso completo (Ejecutar métodos, Escritura completa, Escritura parcial, Escritura de proveedor, Habilitar cuenta, Llamada remota habilitada, Seguridad de lectura y Editar seguridad) para los nombres de espacio WMI siguientes:

- Root\CIMV2
- Root\CIMV2\Applications\Exchange
- Root\MicrosoftExchangeV2

Si el ID de servicio de Windows para la cuenta de servicio de TADDM tiene permisos suficientes para descubrir un servidor de Microsoft Exchange, el sensor utiliza el ID de servicio de Windows y no es necesaria ninguna entrada de lista de acceso de servidor de Microsoft Exchange.

Si el ID de servicio de Windows para la cuenta de servicio de TADDM no tiene suficientes permisos para descubrir un servidor de Microsoft Exchange, debe crear una lista de acceso de servidor de Microsoft Exchange.

Procedimiento

Para configurar la lista de acceso, efectúe los pasos siguientes:

1. En la consola de Discovery Management, cree una definición de ámbito de descubrimiento que incluya su Microsoft Exchange Server, o utilice un ámbito existente que contenga su Microsoft Exchange Server.
2. Para crear una lista de acceso, pulse el icono **Lista de acceso**.
3. En la ventana Lista de acceso, pulse **Añadir**.
4. En el campo **Tipo de componente** de la ventana Detalles de acceso, pulse **Servidores de la aplicación**.
5. En el campo **Proveedor**, pulse **Microsoft Exchange Server**.

6. Escriba las credenciales de Microsoft Exchange Server.

Configuración de servidores VMware:

Si está bien configurado, el proceso de descubrimiento de TADDM devuelve información sobre los de servidores VMware.

Acerca de esta tarea

Para configurar servidores VMware para el descubrimiento, defina los permisos de sólo lectura para la cuenta de servicio que no sea raíz de TADDM en la consola VMware ESX. O bien, puede utilizar el usuario raíz para el descubrimiento. Para obtener más información sobre los servidores VMware, puede buscarla en los temas que aparecen en el panel comunitario de VMware, en la página web https://communities.vmware.com/welcome.

Configuración de bases de datos para el descubrimiento:

Para dar soporte al descubrimiento de las bases de datos, debe crear los usuarios de las bases de datos DB2, Oracle o Sybase para el servidor de TADDM. El servidor de TADDM utiliza estos usuarios de bases de datos para recopilar información sobre las bases de datos que se ejecutan en host remotos.

Creación de un usuario de DB2:

Para descubrir completamente instancias de DB2 en hosts de sistemas remotos, cree un usuario de DB2.

Procedimiento

Para crear un usuario de DB2, efectúe los pasos siguientes:

1. Cree un usuario con acceso a los elementos siguientes:
   - El servidor TADDM de la base de datos DB2
   - Todas las instancias del servidor de TADDM de la base de datos DB2 que deben descubrirse
2. Configure este usuario de DB2 para que tenga acceso SSH al sistema en el que esté alojado el servidor de la base de datos DB2.
3. En la lista de acceso del servidor TADDM, complete los pasos siguientes para añadir el nombre de usuario y la contraseña al usuario de DB2:
   a. En la barra de herramientas de la consola de Discovery Management, pulse **Descubrimiento** > **Lista de acceso**. Se visualiza el panel Lista de acceso.
   b. Pulse **Añadir**. Se visualiza la ventana Detalles de acceso.
   c. En la ventana Detalles de acceso, complete la información siguiente:
      1) En la lista **Tipo de componente**, seleccione **Base de datos**.
      2) En la lista **Proveedor**, seleccione **DB2**.
      3) Especifique el Nombre, el Nombre de usuario y la Contraseña del usuario de DB2.
   d. Pulse **Aceptar** para guardar la información. Se visualiza el panel Lista de acceso con la información nueva.

Creación de un usuario de Microsoft SQL Server:

Para descubrir completamente instancias de Microsoft SQL Server en hosts de sistemas remotos, cree un usuario de Microsoft SQL Server.

Procedimiento

Para crear un usuario de Microsoft SQL Server, efectúe los pasos siguientes:

1. Cree un usuario de Microsoft SQL Server con privilegios de rol de `db_datareader` y permiso `VIEW_ANY_DEFINITION`. Es posible que esta tarea la deba realizar el administrador de Microsoft SQL Server.
2. En la consola de Discovery Management, complete los pasos siguientes para añadir el nombre de usuario y la contraseña al usuario del servidor SQL Microsoft en la lista de acceso del servidor de TADDM:
   a. En la barra de herramientas, pulse **Descubrimiento** > **Lista de acceso**. Se visualiza el panel Lista de acceso.
   b. Pulse **Añadir**. Se visualiza la ventana Detalles de acceso.
   c. En la ventana Detalles de acceso, escriba la información siguiente:
      1) En la lista **Tipo de componente**, seleccione **Base de datos**.
      2) En la lista **Proveedor**, seleccione **Microsoft SQL Server**.
      3) Especifique el **Nombre**, el **Nombre de usuario** y la **Contraseña**.
   d. Pulse **Aceptar** para guardar la información. Se visualiza el panel Lista de acceso con la información nueva.

Creación de un usuario de Oracle:

Para descubrir completamente instancias de Oracle en hosts de sistemas remotos, cree un usuario de Oracle.

Procedimiento

Para crear un usuario de Oracle, efectúe los pasos siguientes:

1. Cree un usuario de Oracle con privilegios SELECT_CATALOG_ROLE. Es posible que esta tarea la deba realizar el administrador de Oracle.

   Por ejemplo, utilice el mandato siguiente para crear el usuario de Oracle de IBM:

   ```
   create user collation identified by collpassword;
   grant connect, select_catalog_role to collation;
   ```
2. En la consola de Discovery Management, complete los pasos siguientes para añadir el nombre de usuario y la contraseña al usuario Oracle en la lista de acceso del servidor de TADDM:
   a. En la barra de herramientas, pulse **Descubrimiento** > **Lista de acceso**. Se visualiza el panel Lista de acceso.
   b. Pulse **Añadir**. Se visualiza la ventana Detalles de acceso.
   c. En la ventana Detalles de acceso, complete la información siguiente:
      1) En la lista **Tipo de componente**, seleccione **Base de datos**.
      2) En la lista **Proveedor**, seleccione **Oracle**.
      3) Especifique el Nombre, el Nombre de usuario y la Contraseña del sistema.
   d. Pulse **Aceptar** para guardar la información. Se visualiza el panel Lista de acceso con la información nueva.

Creación de un usuario de Sybase:

Para descubrir completamente Sybase ASE en hosts de sistemas remotos, cree un usuario de Sybase asignado a un rol apropiado.

Procedimiento

Para crear un usuario de Sybase, efectúe los pasos siguientes:

1. Utilice el mandato siguiente para crear un usuario de Sybase que sea miembro del rol sa.

   ```
   sp_role "grant",sa_role,IBM
   ```

   Asegúrese de que el usuario IQ de Sybase es miembro de DBA. Si el usuario IQ de Sybase no es miembro de DBA, no se puede encontrar la información IQ de Sybase específica de la base de datos.
2. En la consola de Discovery Management, complete los pasos siguientes para añadir el nombre de usuario y la contraseña al usuario Sybase en la lista de acceso del servidor de TADDM:
   a. Para crear una lista de acceso, pulse el icono **Lista de acceso**.
   b. En la ventana Lista de acceso, pulse **Añadir**.
   c. En el campo **Tipo de componente** de la ventana Detalles de acceso, pulse **Base de datos**.
   d. En el campo **Proveedor**, pulse **Base de datos**.
   e. Escriba las credenciales (nombre de usuario y contraseña) para establecer Java Database Connectivity (JDBC) en el servidor Sybase.

Configuración del descubrimiento de sistemas Windows

Para el descubrimiento en sistemas Windows, TADDM da soporte al descubrimiento basado en pasarela y al descubrimiento basado en SSH, así como al descubrimiento asíncrono y basado en scripts.

Para obtener información acerca del descubrimiento asíncrono, consulte “Configuración del descubrimiento asíncrono” en la página 108. Para obtener información acerca del descubrimiento basado en scripts, consulte “Configuración del descubrimiento basado en script” en la página 112.

El descubrimiento basado en pasarela requiere un sistema Windows dedicado, accesible a través de SSH, que sirva de pasarela. Todas las solicitudes de descubrimiento pasan por la pasarela. La pasarela utiliza Windows Management Instrumentation (WMI) para descubrir los sistemas informáticos Windows de destino.

Fix Pack 2 Si utiliza TADDM 7.3.0.2, o posterior, en lugar de WMI, también puede utilizar la sesión PowerShell para descubrir los sistemas Windows de destino. Puede configurar TADDM para que permita la comunicación únicamente mediante la sesión de PowerShell. Para obtener más información, consulte el tema *Configuración para el descubrimiento por medio de un cortafuegos sin un ancla* en la *Guía del usuario* de TADDM.

El descubrimiento basado en SSH no requiere un sistema informático de pasarela dedicado. En su lugar, el descubrimiento utiliza una conexión SSH directa al sistema informático de Windows de destino.

En general, el descubrimiento basado en pasarela es preferible al descubrimiento basado en SSH, porque la configuración de la pasarela y WMI o Powershell es más sencilla que la configuración de SSH. WMI está disponible de forma predeterminada en todos los sistemas de destino Windows a los que da soporte TADDM. PowerShell solo está soportado para destinos que ejecutan Windows Server 2008 y posterior. Debe tener instalado PowerShell versión 2, o posterior, en la pasarela y en los sistemas de destino. Aparte del sistema de pasarela, que requiere un servidor SSH, no hay ningún requisito de software especial para los sistemas de destino Windows. No obstante, realizar el descubrimiento mediante SSH puede ser más rápido porque no hay ninguna pasarela implicada en el flujo de descubrimiento, y no hay necesidad de desplegar el proveedor WMI.

Efectuar un descubrimiento directo requiere un servidor SSH en cada sistema de destino Windows. Además, para un descubrimiento directo mediante SSH, es necesario instalar Microsoft .NET Framework versión 2 o 3 en cada sistema de destino Windows .NET Framework no se instala de forma predeterminada en Windows Server 2000.

Nota: Fix Pack 2 Si utiliza TADDM 7.3.0.2, o posterior, puede instalar también .NET Framework versiones 4 o 4.5.

Para ambos tipos de descubrimiento, el programa de descubrimiento de TADDM deWindows, archivo TaddmTool.exe, se utiliza para realizar el descubrimiento. Para realizar un descubrimiento utilizando una pasarela, el programa TaddmTool se despliega en la pasarela durante la inicialización del descubrimiento. Para realizar descubrimiento utilizando SSH, el programa TaddmTool se despliega en cada sistema informático de destino de Windows. El programa TaddmTool es una aplicación .NET.

De forma predeterminada, TADDM se configura para utilizar solamente el descubrimiento basado en pasarela. Esta configuración se controla siguiendo dos propiedades del servidor TADDM, que se describen en el documento *Referencias de sensores* de TADDM para el sensor del sistema Windows.

- `com.collation.AllowPrivateGateways=true`
- `com.collation.PreferWindowsSshOverGateway=false`

De forma predeterminada, TADDM se configura para utilizar la sesión WMI. Para obtener información de cómo utilizar la sesión PowerShell y cómo habilitarla, consulte “Sesión PowerShell” en la página 132.

Tanto si utiliza una pasarela de Windows con WMI como si utiliza una conexión directa con SSH, la información que se recupera es idéntica. La siguiente lista identifica los requisitos previos para descubrimientos basados en pasarela y en SSH:

Requisitos previos para el descubrimiento basado en pasarela con WMI

1. Se requiere un sistema de Windows Server dedicado para que sirva de pasarela. Los requisitos del sistema operativo para los servidores de pasarela son los mismos que los requisitos del sistema operativo Windows para servidores TADDM. Para obtener detalles sobre los sistemas operativos Windows admitidos, consulte el tema *Requisitos de software del servidor de TADDM* en la *Guía de instalación* de TADDM.
2. La pasarela debería estar en la misma zona de cortafuegos que los sistemas Windows que deben descubrirse.

3. Debe instalar una versión soportada de un servidor SSH en el sistema informático de pasarela.
4. La pasarela utiliza WMI remoto para descubrir cada destino de Windows. Además, se despliega automáticamente un proveedor WMI en cada sistema informático de destino de Windows durante la inicialización del descubrimiento. El proveedor WMI se utiliza para descubrir datos que no están incluidos en la WMI principal. Habilite WMI en el sistema informático de destino de Windows que se va a descubrir. De forma predeterminada, en la mayoría de sistemas Windows 2000 y posteriores, WMI está habilitada.

Fix Pack 2 **Requisitos previos para el descubrimiento basado en pasarela con PowerShell**

1. Se requiere un sistema de Windows Server dedicado para que sirva de pasarela. Los requisitos del sistema operativo para los servidores de pasarela son los mismos que los requisitos del sistema operativo Windows para servidores TADDM. Para obtener detalles sobre los sistemas operativos Windows admitidos, consulte el tema *Requisitos de software del servidor de TADDM* en la *Guía de instalación* de TADDM.
2. Debe instalar PowerShell versión 2, o posterior, en la pasarela y en los sistemas de destino. Solo está soportado los destinos que ejecutan Windows Server 2008, o posterior.
3. Debe configurar la pasarela ejecutando el mandato siguiente:

   ```
   Set-Item WSMan:\localhost\Client\TrustedHosts * -Force
   ```

   Este mandato establece la lista **trustedHosts**. De forma predeterminada, la lista existe pero está vacía y se debe establecer antes de abrir la sesión remota. Con el parámetro `-Force`, PowerShell ejecuta el mandato sin realizar ninguna solicitud para cada paso.
4. Debe configurar los sistemas de destino ejecutando el siguiente mandato:

   ```
   Enable-PSRemoting -Force
   ```

   Este mandato inicia el servicio WinRM, los establece para que se inicie automáticamente con el sistema y crea una regla de cortafuegos para permitir las conexiones de entrada. Con el parámetro `-Force`, PowerShell ejecuta estas acciones sin realizar ninguna solicitud para cada paso.

Requisitos previos para el descubrimiento basado en SSH

1. Es necesario instalar una versión soportada de un servidor SSH en cada sistema de destino Windows.
2. Debe instalar Microsoft .NET Framework versión 2 o 3 en cada sistema de destino de Windows Server.

   Nota: Fix Pack 2 Si utiliza TADDM 7.3.0.2, o posterior, también puede instalar .NET Framework versiones 4 o 4.5.

Consulte también el tema *Configuración para un descubrimiento de Windows no de administrador* de la *Referencia de sensores* de TADDM.

Configuración de Bitvise WinSSHD

Puede utilizar Bitvise WinSSHD para proporcionar acceso SSH a sistemas Windows.

Antes de empezar

Para el descubrimiento basado en pasarela, se tiene que haber instalado Bitvise WinSSHD en el sistema que haga de pasarela. Para el descubrimiento SSH directo, Bitvise WinSSHD debe instalarse en cada sistema Windows.

Para obtener más información sobre las versiones admitidas de Bitvise WinSSHD, consulte el tema *Pasarelas Windows* en la *Guía de instalación* de TADDM.

Bitvise WinSSHD está disponible en la página web http://www.bitvise.com/.

Acerca de esta tarea

En los siguientes pasos se describe cómo configurar Bitvise WinSSHD 5.22. Los pasos específicos pueden variar en función del release de Bitvise WinSSHD de que disponga.

Procedimiento

1. Para restringir el acceso del host SSH al servidor de TADDM, lleve a cabo los siguientes pasos:
   a. En WinSSHD Control Panel, pulse **Open easy settings**.
   b. En el separador **Server settings**, del campo **Open Windows Firewall**, seleccione **As set in Advanced WinSSHD settings**.
   c. Pulse **Save Changes**.
   d. En WinSSHD Control Panel, pulse **Edit advanced settings**. Se muestra la ventana Advanced WinSSDH Settings.
   e. Pulse **Settings** > **Session**.
   f. Establezca el valor de los siguientes elementos como `0`:
      - Bloqueo de IP - duración de ventana
      - Bloqueo de IP - tiempo de cierre
   g. Pulse **Aceptar**.
   h. En WinSSHD Control Panel, pulse **Edit advanced settings**. Se muestra la ventana Advanced WinSSDH Settings.
   i. Pulse **Settings** > **Access Control**.
   j. En el panel derecho, pulse **IP rules**.
   k. Pulse **Añadir**.
   l. Escriba la dirección IP del servidor de TADDM.
   m. En el campo **Number of significant bits**, escriba `32`.
   n. En el campo **Description**, escriba `servidor de TADDM`.
   o. Asegúrese de que la casilla de verificación **Allow connect** está seleccionada.
   p. Pulse **Aceptar**.
   q. Elimine la entrada `0.0.0.0/0` de la lista.
2. Para crear y configurar usuarios y grupos virtuales, lleve a cabo los siguientes pasos:
   a. En WinSSHD Control Panel, pulse **Edit advanced settings**. Se muestra la ventana Advanced WinSSDH Settings.
   b. Pulse **Settings** > **Virtual Groups**.
   c. Para añadir un grupo, pulse **Add**.
   d. En los campos **Group** y **Windows Account Name**, escriba un nombre.

e. Pulse **Aceptar**.
f. Pulse **Settings** > **Virtual Accounts**.
g. Para añadir una cuenta, pulse **Add**.
h. En el campo **Virtual account name**, escriba un nombre.
i. Establezca una contraseña utilizando el enlace de la contraseña de la cuenta virtual.
j. En la lista desplegable, seleccione el grupo virtual que ha creado en un paso anterior y asegúrese de que la casilla de verificación **Use group default Windows account** está seleccionada.
k. Pulse **Aceptar**.

3. En WinSSHD Control Panel, pulse **Start WinSSHD**.

Qué hacer a continuación

Si se descubren varios servidores Windows, es posible que se reciba el mensaje siguiente:

```
No se puede encontrar una pasarela en funcionamiento
```

Para obtener más información sobre configuración adicional que pueda servir de ayuda, consulte el tema *Problemas de pasarelas* en la *Guía de resolución de problemas* de TADDM.

Configuración del daemon Cygwin SSH

Puede utilizar el daemon Cygwin SSH (sshd) para proporcionar acceso SSH a sistemas Windows.

Acerca de esta tarea

Para el descubrimiento basado en pasarela, se tiene que haber instalado Bitvise WinSSHD en el sistema que haga de pasarela; para el descubrimiento SSH directo, el daemon debe instalarse en cada sistema Windows.

Para obtener más información sobre las versiones admitidas de deaemon Cygwin SSH, consulte el tema *Pasarelas Windows* en la *Guía de instalación* de TADDM.

Importante: Para que el descubrimiento mediante Cygwin SSH se realice correctamente, se deben cumplir los requisitos siguientes:

- Se da soporte a anclas y pasarelas en Cygwin, edición de 64 bits, en Windows Server 2012 x64 y Windows Server 2008 x64.
- El usuario del descubrimiento y el usuario que inicia el servicio deben ser el mismo. El usuario del descubrimiento debe ser miembro del grupo de administradores.

Cygwin está disponible en la página web http://www.cygwin.com/.

Procedimiento

Para configurar del daemon Cygwin SSH:

1. Inicie la shell cygwin bash.
2. En la información del sistema, utilice el programa de utilidad **cygwin mkpasswd** para crear un archivo `/etc/passwd` inicial. También puede utilizar el programa de utilidad **mkgroup** para crear un grupo `/etc/` inicial. Para conocer más detalles, consulte la publicación *Cygwin User's Guide*.

Por ejemplo, el mandato siguiente configura el archivo de contraseña, `passwd`, desde las cuentas locales en el sistema:

```
mkpasswd -l > /etc/passwd
```

3. Ejecute el programa de configuración ssh-host-config.
4. Configure SSH. Responda `Sí` a todas las preguntas.
5. Inicie el servidor SSH ejecutando el mandato siguiente:

```
net start sshd
```

Qué hacer a continuación

El servicio Cygwin (sshd) debe utilizar una cuenta de usuario de dominio administrativo al acceder al servidor de pasarela. Esta cuenta de usuario es necesaria para algunos sensores, por ejemplo, el sensor de Microsoft Exchange. Efectúe los pasos siguientes:

1. Configure la cuenta de usuario de dominio ejecutando los mandatos siguientes:

```
mkpasswd -u [domain_user] -d [domain] >> /etc/passwd
mkgroup -d [domain] >> /etc/group
```

2. Inicie el programa services.msc. Compruebe las propiedades de inicio de sesión para el servicio Cygwin (sshd) que se creó. Verifique que el servicio está configurado para ser ejecutado por una cuenta de usuario de dominio administrativo.
3. Los archivos de configuración y registro de Cygwin (sshd) deben pertenecer a la misma cuenta de usuario de dominio que utiliza el servicio de Cygwin (sshd) para acceder a la pasarela. Ejecute los mandatos siguientes:

```
$ chown [domain_user] /var/log/sshd.log
$ chown -R [domain_user] /var/empty
$ chown [domain_user] /etc/ssh*
```

4. La cuenta de usuario de dominio debe tener los siguientes permisos en el servidor de pasarela:
   - Ajuste las cuotas de memoria para un proceso
   - Cree un objeto de señal
   - Inicie sesión como un servicio
   - Sustituya una señal a nivel de proceso

Si se descubren varios servidores Windows, es posible que se reciba el mensaje siguiente:

```
No se puede encontrar una pasarela en funcionamiento
```

Para obtener más información sobre configuración adicional que pueda servir de ayuda, consulte el tema *Problemas de pasarela* en la *Guía de resolución de problemas* de TADDM.

Configuración de Remotely Anywhere

Puede utilizar Remotely Anywhere para proporcionar acceso SSH a sistemas Windows.

Acerca de esta tarea

Para obtener más información sobre las versiones admitidas de Remotely Anywhere, consulte el tema *Pasarelas Windows* en la *Guía de instalación* de TADDM.

Para el descubrimiento basado en pasarela, se tiene que haber instalado Remotely Anywhere en el sistema que actúa como pasarela.

Para el descubrimiento SSH directo, Remotely Anywhere debe instalarse en cada sistema Windows.

Puede utilizar los valores de configuración predeterminados en Remotely Anywhere. Para obtener más información, vaya a http://remotelyanywhere.com/.

Configuración del servidor Tectia SHH

Puede utilizar el servidor Tectia SSH para proporcionar acceso SSH a los sistemas Windows.

Acerca de esta tarea

Para obtener más información sobre las versiones soportadas del servidor Tectia SSH, consulte el tema *Pasarelas Windows* en la *Guía de instalación* de TADDM.

Para el descubrimiento basado en pasarela, se tiene que haber instalado el servidor Tectia SSH en el sistema de pasarela.

Para el descubrimiento de SSH directo, el servidor Tectia SSH debe haberse instalado en cada uno de los sistemas Windows.

Puede utilizar los valores de configuración predeterminados en el servidor Tectia SSH. Para obtener más información, vaya a http://www.ssh.com.

Dependencia de Windows Management Instrumentation (WMI)

TADDM se basa en Windows Management Instrumentation (WMI) para descubrir los sistemas Windows. TADDM puede configurarse para que reinicie el servicio WMI, si se produce algún problema con WMI. Si el servicio de WMI se ha reiniciado, también se reinician todos los servicios dependientes de WMI que estaban en ejecución antes del reinicio.

Las siguientes propiedades del servidor de TADDM controlan el reinicio de WMI.

Nota: El valor predeterminado para el reinicio de WMI es `false`. Establecer los valores de las propiedades siguientes en `true` puede proporcionar un descubrimiento en Windows más fiable, pero debe tener en cuenta también el posible impacto negativo que puede producir la detención y el reinicio temporales del servicio WMI.

- `com.collation.RestartWmiOnAutoDeploy=false`
- `com.collation.RestartWmiOnAutoDeploy.1.2.3.4=false`
- `com.collation.RestartWmiOnFailure=false`
- `com.collation.RestartWmiOnFailure.1.2.3.4=false`

Para obtener más información sobre las propiedades del servidor de TADDM que utiliza el sensor de sistemas Windows, consulte el tema *Configuración del archivo collation.properties* en el apartado de sensores de sistema Windows de la *Referencia de sensores*.

Sesión PowerShell

Fix Pack 2

Para descubrir sistemas Windows, puede utilizar WMI o la sesión PowerShell. En comparación con la sesión WMI, en la sesión PowerShell TADDM envía menos solicitudes para acceder a los sistemas de destino, que disminuye el número de sucesos que se registran. La sesión PowerShell solo se puede utilizarla con los

sensores basados en scripts. Si desea iniciar utilizando la sesión PowerShell, debe habilitarla por que está inhabilitada de forma predeterminada.

Puede utilizar ambas sesiones al mismo tiempo. Si está ejecutando descubrimientos normales o basados en scripts, no puede inhabilitar la sesión WMI por el descubrimiento normal falla sin ella. Sin embargo, puede dar prioridad al uso de la sesión PowerShell.

Importante: Si solo ejecuta descubrimientos normales, no se da soporte a la sesión PowerShell.

Puede controlar el uso y prioridad de la sesión PowerShell utilizando las propiedades siguientes:

- `com.collation.PowerShellAccessEnabled=false`
- `com.collation.WmiAccessEnabled=true`
- `com.collation.PreferPowerShellOverWMI=true`
- `com.collation.PowerShellPorts=5985,5986`
- `com.ibm.cdb.session.ps.useSSL=false`
- `com.ibm.cdb.session.ps.allowDNS=true`
- `com.ibm.cdb.session.ps.fallbackToIP=true`
- `com.collation.PowerShellTimeoutFudge=10000`
- Fix Pack 3 `com.ibm.cdb.session.ps.urlPrefix=wsman`

Para habilitar la sesión PowerShell, establezca la propiedad `com.collation.PowerShellAccessEnabled` en `true`. De forma predeterminada, se prefiere la sesión PowerShell sobre la sesión WMI.

Para obtener más información acerca de estas propiedades, consulte *Configuración de las entradas del archivo `collation.properties`* para el sensor del sistema Windows en el *Manual de consulta del sensor* de TADDM.

Nota: En un caso muy concreto, al configurar el cortafuegos para permitir la comunicación solo mediante una sesión de PowerShell, debe abrir los puertos de PowerShell y configurar la propiedad del sensor Ping. Para obtener más información, consulte el tema *Configuración para el descubrimiento por medio de un cortafuegos sin un ancla* en la *Guía del usuario* de TADDM.

Casos de uso de ejemplo

En función de cómo descubra sus sistemas de destino Windows, puede configurar las propiedades anteriores de los modos siguientes.

- Está utilizando únicamente los sensores que dan soporte al descubrimiento basado en scripts. En este caso, puede habilitar la sesión PowerShell estableciendo la propiedad `com.collation.PowerShellAccessEnabled` en `true` e inhabilitar la sesión WMI estableciendo la propiedad `com.collation.WmiAccessEnabled` en `false`. Sin embargo, cuando PowerShell no está disponible, la sesión y el descubrimiento fallan.
- Está utilizando sensores que dan soporte al descubrimiento normal y basado en scripts. En este caso, no inhabilite la sesión WMI, ya que hará que falle el descubrimiento normal. Habilite la sesión PowerShell estableciendo la propiedad `com.collation.PowerShellAccessEnabled` en `true`. Para establecer la sesión PowerShell, siempre que sea posible, no cambie el valor predeterminado de la propiedad `com.collation.PreferPowerShellOverWMI`. En este caso, TADDM crea

una sesión híbrida que puede utilizar las funciones PowerShell y WMI. La sesión WMI solo se utiliza cuando la sesión PowerShell no puede ejecutar las tareas que solicitan los sensores normales.

Configuración del descubrimiento de marcadores de posición

Fix Pack 3

Puede configurar TADDM para crear marcadores de posición para dependencias no descubiertas de la infraestructura.

El marcador de posición es un objeto que forma parte de la infraestructura, pero que no está representado en TADDM con los valores predeterminados. Los motivos por lo que no se representa pueden ser que una parte de la conexión no está descubierta, que ningún sensor da soporte a tal tipo de objeto, o que no hay creada ninguna plantilla de servidor personalizada.

Los marcadores de posición son de la clase SSoftwareServer. Tienen establecidos los atributos `hierarchyDomain` e `hierarchyType`. La tabla siguiente especifica los valores de los atributos:

Tabla 35. Valores de los atributos `hierarchyDomain` e `hierarchyType`.

Lado de conexión	**Valor del atributo `hierachyDomain`**	**Valor del atributo `hierarchyType`**
Local	`app.placeholder.client.local`	Nombre del mandato que origina la conexión, por ejemplo `Java`
Remoto	`app.placeholder.server.remote`	`Desconocido`

Con el uso de estos valores, puede filtrar relaciones no deseadas en la configuración de cruce de las aplicaciones empresariales. Para obtener detalles, consulte el tema *Configuración de cruce* de la *Guía del usuario* de TADDM.

Cuando se crea un marcador de posición y, a continuación, un sensor crea el Servidor de aplicaciones equivalente, o una plantilla de servidor personalizada, el PlaceholderCleanupAgent fusiona el marcador de posición con el Servidor de aplicaciones descubierto.

Nota: Puede crear marcadores de posición en TADDM 7.3.0.2, pero está limitado. Por lo tanto, se recomienda utilizar marcadores de posición en TADDM 7.3.0.3 y posterior. La migración de marcadores de posición creados de FP2 a FP3 no está soportada.

Habilitación de la creación de marcadores de posición

Para habilitar la creación de marcadores de posición, añada la propiedad siguiente en el archivo `collation.properties`:

```
com.ibm.cdb.topomgr.topobuilder.agents.ConnectionDependencyAgent2
dependencyPlaceholders=true
```

El valor predeterminado es `false`.

Cuando establezca esta propiedad en `true` por primera vez, debe reiniciar TADDM para habilitar los atributos ampliados para las clases LogicalConnection y SoftwareServer. Estos atributos ampliados son necesarios para el correcto funcionamiento de esta característica.

En caso de que la propiedad anterior se establezca en `true` no hay necesidad de establecer explícitamente las propiedades siguientes en `collation.properties`, sino que se utilizarán sus valores codificados.

```
com.ibm.taddm.dependencyPlaceholders.create.localClient.to.remoteServer
=true
```

El valor predeterminado es `true`.

```
com.ibm.taddm.dependencyPlaceholders.create.remoteClient.to.localServer
=false
```

El valor predeterminado es `false`.

Nota: Se puede cambiar el comportamiento de las variables estableciendo estas propiedades en `collation.properties`.

Importante: Cuando habilite la creación de marcadores de posición, las aplicaciones empresariales podrían crecer significativamente y el proceso de construcción podría llevar más tiempo. Para impedirlo, puede filtrar relaciones no deseadas en la configuración de cruce de las aplicaciones empresariales.

Visualización de marcadores de posición

Puede ver los marcadores de posición en el panel Resumen de inventario una vez que establezca el filtro en `Placeholders`. Los marcadores de posición para dependencias no descubiertas se encuentran en el separador **Servidores de software**.

Creación de plantillas de servidor personalizado

Puede utilizar marcadores de posición para crear plantillas de servidor personalizado de las formas siguientes:

- Utilizando la información sobre marcadores de posición generada por la herramienta `bizappscli`. Para obtener detalles, consulte el tema *Acciones para analizar el contenido de las aplicaciones empresariales* de la *Guía del usuario* de TADDM.
- Utilizando la información de línea de mandatos que se muestra en el separador **Tiempo de ejecución** del panel Detalles para los marcadores de posición de tipo `app.placeholder.*.local`.

Para obtener más información sobre las plantillas de servidor personalizadas, consulte el tema *Creación y gestión de plantillas de servidor personalizado* de la *Guía del usuario* de TADDM.

Creación de servidores de aplicaciones de nivel 3 sin credenciales

Fix Pack 2

Si desea descubrir información básica de nivel 3 sobre los elementos de su infraestructura, no es necesario que proporcione las credenciales en la lista de acceso. Puede crear servidores de aplicaciones mediante plantillas internas de sensor. CustomAppServerTopoAgent puede procesar dichas plantillas o las puede procesar un sensor de plantillas de servidor durante un descubrimiento.

Acerca de esta tarea

Al crear servidores de aplicaciones sin credenciales puede descubrir solo información básica sobre su infraestructura, por ejemplo, qué tipo de software se instala. Elija esta modalidad si no desea proporcionar el descubrimiento de nivel 3, pero desea descubrir información básica sobre su infraestructura.

Existen dos métodos para crear servidores de aplicaciones de nivel 3. Puede ejecutar un sensor de plantillas de servidor o habilitar CustomAppServerTopoAgent.

Procedimiento

- Ejecute un descubrimiento con un sensor de plantillas de servidores
  Efectúe los pasos siguientes:
  1. En el archivo `collation.properties`, establezca la propiedad `com.collation.internaltemplatesenabled` en `true`. Esta propiedad habilita plantillas internas de sensores de nivel 3. El valor predeterminado es `false`.
  2. Ejecute el descubrimiento mediante un perfil que no contenga el sensor que normalmente descubre la información que desea descubrir mediante un sensor de plantillas personalizado. Por ejemplo, si desea descubrir información básica para el servidor de DB2, elija el descubrimiento del perfil de nivel 2, o un perfil propio que no contenga un servidor de IBM DB2. Si el perfil contiene un sensor de IBM DB2, se ejecuta dicho sensor en lugar del sensor de plantillas de servidor.
- Ejecute CustomAppServerTopoAgent
  CustomAppServerTopoAgent utiliza procesos de tiempo de ejecución descubiertos previamente por el sensor de servidores genéricos. Puede ejecutar el agente manualmente o establecerlo para que se ejecute automáticamente. Efectúe los pasos siguientes:
  1. Tanto para la modalidad manual como para la modalidad automática del agente, en el archivo `collation.properties`, establezca la propiedad `com.collation.internaltemplatesenabled` en `true`. Esta propiedad habilita plantillas internas de sensores de nivel 3. El valor predeterminado es `false`.
  2. Para iniciar manualmente CustomAppServerTopoAgent, ejecute el mandato:
     ```
     COLLATION_HOME/support/bin/runtopobuild.sh -a CustomAppServerTopoAgent
     ```
  3. Para configurar ejecuciones automáticas del agente, establezca la propiedad `com.ibm.cdb.topobuilder.groupinterval.discovery=` en el archivo `collation.properties`.
     Esta propiedad especifica la periodicidad con la que se ejecuta el agente. De forma predeterminada no se proporciona ningún valor, lo que significa que el agente se inhabilita. Para habilitarlo, especifique el valor en horas, por ejemplo `com.ibm.cdb.topobuilder.groupinterval.discovery=4`.
- Opcional: Seleccione plantillas para excluirlas del procesamiento
  Si desea habilitar solo algunas plantillas internas de sensores de nivel 3, puede controlarlo con la propiedad siguiente:
  ```
  com.collation.discovery.ignoreTemplateList
  ```

  Esta propiedad especifica una lista de plantillas internas que no desea procesar. El valor de esta propiedad es una lista separada por puntos y coma por ejemplo `com.collation.discovery.ignoreTemplateList=DB2Unix;MSSQL`. Puede buscar el nombre de una plantilla interna en el Portal de gestión de datos del campo **Nombre de objeto**, que encontrará en el separador **General** del panel **Detalles** de **Otros servidores de bases de datos**.

Configuración de etiquetado de ubicación

El etiquetado de ubicación indica dónde se ha creado cada elemento de configuración (CI). Activa el filtrado basado en ubicaciones de los elementos de configuración en informes BIRT y consultas de API.

Si habilita el etiquetado de ubicación, cada objeto descubierto almacenado en la base de datos de descubrimiento incluye el atributo **locationTag** (serie). Los objetos, como las relaciones, los objetos de agregación y los objetos heredados creados mediante agentes de topología, incluyen los datos de etiquetas de ubicación en determinados casos:

- Una relación uno a uno (por ejemplo, Dependency o NetworkConnection) incluye una etiqueta de ubicación si la ubicación es la misma para ambos objetos conectados.
- Un objeto de agregación (por ejemplo, un clúster) incluye una etiqueta de ubicación si la ubicación es la misma para todos los objetos agregados.

  Nota: En el caso de las colecciones personalizadas, el atributo **locationTag** sólo se establece cuando el *valor* de la etiqueta de ubicación de todos los CI principales de la colección personalizada es el mismo. Cuando la colección personalizada se amplía con un CI principal que tiene una etiqueta de ubicación diferente, el atributo **locationTag** para dicha colección personalizada se borra.
- Un objeto simple incluye la etiqueta de ubicación del objeto en el que se basa.

En todos los demás casos, los objetos creados mediante agentes de topología no incluyen un valor de etiqueta.

Para habilitar el etiquetado de ubicación, configure la siguiente propiedad en el archivo `collation.properties`:

```
com.ibm.cdb.locationTaggingEnabled=true
```

Los valores del etiquetado de ubicación pueden ser estáticos (especificados en un determinado servidor o ancla) o dinámicos (especificados para un determinado descubrimiento o importación de libros IdML). Los valores del etiquetado de ubicación no pueden sobrepasar los 192 caracteres. Si la etiqueta especificada supera los 192 caracteres, se corta para que se ajuste a la longitud necesaria.

Limitaciones

Cuando se ejecuta un descubrimiento de Nivel N1, los elementos de configuración que ya están presente en la base de datos no se actualizan. Como resultado, las etiquetas de ubicación se asignan solo a los objetos recién descubiertos.

Etiquetado de ubicación estático

El etiquetado de ubicación estático asigna el atributo **locationTag** a todos los objetos descubiertos o cargados mediante la importación de libros IdML en función de la configuración estática del TADDM o el servidor ancla.

Servidor de TADDM

Para configurar el valor de etiqueta de ubicación de los CI creados en un servidor de TADDM, especifique la siguiente propiedad en el archivo `collation.properties`:

```
com.ibm.cdb.locationTag=location
```

donde **location** es el valor de etiqueta de ubicación que desea utilizar.

Ancla

Para configurar el valor de etiqueta de ubicación de los CI creados en un ancla, configure el atributo **anchor_location_n** en el archivo `$COLLATION_HOME/etc/anchor.properties`. Las siguientes entradas de ejemplo del archivo `anchor.properties` indican la forma en que están configurada la información de ubicación para las anclas:

```
anchor_host_1=192.168.1.13
anchor_scope_1=FIRST_SCOPE
anchor_zone_1=FIRST_ZONE
anchor_location_1=FIRST_LOCATION
anchor_host_2=192.168.2.22
anchor_scope_2=SECOND_SCOPE
anchor_location_2=SECOND_LOCATION
Port=8497
```

Si no se ha especificado una etiqueta de ubicación para un ancla, la ubicación de cada uno de los CI creados en el ancla se establece en la ubicación que se ha especificado para el servidor de TADDM al que están conectados los CI.

Si el valor de etiqueta de ubicación no se ha especificado para el ancla o el servidor de TADDM, no se establece ninguna información de ubicación para ese CI.

Etiquetado de ubicación dinámico

El etiqueta de ubicación dinámico establece el atributo **locationTag** mediante un valor especificado para un determinado descubrimiento o importación de libros IdML.

Descubrimiento

Para especificar un valor de etiqueta de ubicación durante el descubrimiento, inicie el descubrimiento desde la línea de mandatos y especifique la etiqueta de ubicación mediante la opción **-l** o **-myLocation**, como en el siguiente ejemplo:

```
api.sh -u administrator -p collation discover start -n discovery1 -p myProfile -l myLocation myScope
```

donde **locationTag** es el valor de etiqueta de ubicación que desea utilizar. El valor que especifique sustituirá cualquier valor de etiqueta estático para los objetos creados durante este descubrimiento específico.

Nota: Si el etiquetado de ubicación no está habilitado en el archivo `collation.properties`, al especificar una etiqueta de ubicación durante el descubrimiento, se producirá una excepción de descubrimiento.

Importación de libros IdML

Para especificar un valor de etiqueta de ubicación al importar un libro IdML, especifique la etiqueta de ubicación mediante la opción -l optativa, como en el siguiente ejemplo:

```
loadidml.sh -f idml_book.xml -l locationTag
```

donde **locationTag** es el valor de etiqueta de ubicación que desea utilizar. Si desea importar varios libros IdML con distintas etiquetas de ubicación, cada libro se debe cargar por separado.

Lista de acceso

Puede crear entradas de lista de acceso con una ubicación asignada.

El atributo de la etiqueta de ubicación es obligatorio, pero se puede modificar posteriormente. Las credenciales se filtran por ubicación; por eso, solo se utilizan las entradas de acceso de determinadas ubicaciones. Esto limita la posibilidad de sustraer la contraseña de otros clientes o ubicaciones. Si ejecuta un descubrimiento sin una etiqueta de ubicación, no se utilizará ninguna de las credenciales etiquetadas.

Cuando se añade una nueva entrada de acceso con la etiqueta de ubicación establecida en el carácter de asterisco (*), se utiliza como la última entrada de acceso que se intenta durante un descubrimiento mientras se establece una sesión con el punto final.

El carácter de asterisco (*) es el valor predeterminado y puede modificarse estableciendo el parámetro siguiente:

```
com.ibm.cdb.locationTag.global=GLOBAL
```

En tal caso, la entrada de acceso con la etiqueta `GLOBAL` es la última que se intenta cuando se ejecuta un descubrimiento. La etiqueta de ubicación anterior sólo se utiliza para la lista de acceso y no tiene influencia en las etiquetas de ubicación asignadas a los CI que se han descubierto durante un descubrimiento.

Informes BIRT

Los informes Business Intelligence and Reporting Tools (BIRT) se pueden filtrar para generar los datos de ubicación específica de clientes.

Si se activa el etiquetado de ubicación, el campo de texto se encuentra en el panel de informes BIRT debajo de la lista de informes. Puede ejecutar un informe BIRT para una etiqueta de ubicación para ver los datos que pertenecen solo a esa ubicación.

Ninguno de los informes preconfigurados puede gestionar etiquetas de ubicación. Si necesita utilizar los informes BIRT, deberá actualizarlos de forma manual para que admitan el filtrado por etiqueta de ubicación.

Mantenimiento y ajuste

Para maximizar el rendimiento de TADDM, es conveniente realizar algunos pasos de configuración adicionales y ciertas tareas de mantenimiento continuo.

Ajuste de los parámetros de carga masiva

Puede personalizar el comportamiento del cargador masivo especificando parámetros concretos en el tiempo de ejecución o configurando el archivo`bulkload.properties`.

Existen tres fases distintas de carga de datos mediante el Cargador masivo:

1. Analizar los objetos y las relaciones para determinar los gráficos en los datos.
   Normalmente, 1 - 5% del tiempo de ejecución
2. Crear los objetos de modelo y los gráficos.
   Normalmente, 2 - 5% del tiempo de ejecución
3. Pasar los datos al servidor de la interfaz de programación de aplicaciones (API).

Normalmente, 90 - 99% del tiempo de ejecución

Existen dos opciones para cargar los datos:

- Los datos pueden cargarse un registro cada vez. Este es el modo predeterminado. Debe cargar los registros de uno en uno para los siguientes archivos:
  - Archivos con errores.
  - Archivos con atributos ampliados.
- Los datos pueden cargarse de forma masiva. Esto se denomina grabación de gráficos, porque se carga un gráfico completo, en lugar de un solo registro.

  La carga masiva con la opción de grabación de gráficos es más rápida que la carga de archivo por archivo. (Consulte la sección sobre las mediciones de la carga masiva para obtener detalles). El siguiente ejemplo muestra la opción de grabación de gráficos, donde -g=almacenamiento intermedio y los bloques de datos se transfieren al servidor de la API:

  ```
  ./loadidml.sh –g –f /home/configia/testfiles/sample.xml
  ```

  Los parámetros siguientes del archivo `bulkload.properties` se pueden utilizar para mejorar el rendimiento al cargar los datos de forma masiva:

  ```
  com.ibm.cdb.bulk.cachesize=2000
  ```

  El parámetro `cachesize` controla el número de objetos procesados en una única operación de grabación cuando se cargan datos de forma masiva con la opción de grabación de gráficos. Aumentar el valor del tamaño de memoria caché mejora el rendimiento, a riesgo de agotar la memoria del cliente o del servidor. Modifique solo el número cuando haya información específica disponible que indique que el procesamiento de un archivo con una memoria caché mayor proporciona ventajas en el rendimiento. El valor predeterminado del tamaño de memoria caché es 2000, y el valor máximo del tamaño de memoria caché es 40000.

  ```
  com.ibm.cdb.bulk.allocpoolsize=1024
  ```

  Este valor especifica la memoria máxima que se puede asignar al proceso del cargador masivo. Se trata de un valor Xmx que se transfiere a la clase Java principal del cargador masivo. Especifique el valor en megabytes.

  Asegúrese de que una máquina virtual Java no se está quedando sin memoria. Puede hacerlo mediante la recopilación de volcados de hebras de procesos de TADDM y su revisión. Si es necesario, aumente el tamaño de la memoria.

  Consejo: Las pruebas ejecutadas en el libro ITNMIP indican que el rendimiento es óptimo cuando se establecen las propiedades y los parámetros del proceso de carga masiva en los valores siguientes:

  ```
  com.ibm.cdb.bulk.cachesize=4000
  com.ibm.cdb.bulk.allocpoolsize=4096
  value-Xms768M|-Xmx1512M|-DTaddm.xmx64=6g|
  ```

  También es importante que ejecute el mandato **RUNSTATS** con frecuencia durante el proceso de carga masiva.

Mantenimiento de la base de datos

Para mantener el rendimiento óptimo del sistema, debe planificar y realizar regularmente mantenimiento y ajustes periódicos de la base de datos de TADDM.

Configuraciones predeterminadas de la base de datos

Las configuraciones de base de datos predeterminadas que se proporcionan con TADDM resultan suficientes como prueba de concepto, prueba de tecnología y pequeñas implementaciones piloto de TADDM.

Directrices de ajustes para las bases de datos DB2 y Oracle

Las siguientes directrices de ajuste se aplican tanto a las bases de datos de DB2 como de Oracle:

1. No trate de limitar el número de unidades físicas de disco disponibles para la base de datos, únicamente en función de la capacidad de almacenamiento.
2. Lo más conveniente sería colocar los componentes siguientes en unidades de disco o matrices separadas:
   - Datos de aplicación (como, por ejemplo, las tablas y los índices)
   - Registros de la base de datos
   - Espacio temporal de la base de datos: se utiliza para las operaciones de clasificación y unión
3. Utilice los discos más rápidos disponibles para los archivos de registro.
4. Habilite la E/S asíncrona a nivel de sistema operativo.

Para obtener más información sobre el ajuste de la base de datos de DB2 y Oracle, consulte *Ajuste de rendimiento de la base de datos en AIX* en http://www.redbooks.ibm.com/redbooks/pdfs/sg245511.pdf.

Para obtener más información sobre el ajuste de la base de datos DB2, consulte también *Relational Database Design and Performance Tuning for DB2 Database Servers* (ajuste de rendimiento y diseño de bases de datos relacionales para servidores de la base de datos DB2) en http://www-01.ibm.com/support/docview.wss?uid=tss1wp100764 y *DB2 UDB Version 8 Product Manuals* (manuales de productos de versión 8 de UDB de DB2) en http://www.ibm.com/support/docview.wss?rs=71&uid=swg27009554.

Supresión de los registros de base de datos antiguos

El número de registros de datos de las tablas crece con el tiempo y según la cantidad de espacio de almacenamiento disponible es preciso que elimine de vez en cuando datos manualmente para que las tablas sigan teniendo un tamaño razonable. Después de eliminar la tabla CHANGE_HISTORY_TABLE, puede eliminar las entradas correspondientes en la tabla CHANGE_CAUSE_TABLE. También puede mejorar el rendimiento y la usabilidad de la herramienta de integridad de los datos si elimina registros antiguos de la tabla ALIASES_JN.

Eliminación de registros de las tablas CHANGE_HISTORY_TABLE y CHANGE_CAUSE_TABLE:

Puede eliminar los registros antiguos para mejorar el rendimiento y mantener las tablas con un tamaño pequeño. Después de eliminar los registros de la tabla CHANGE_HISTORY_TABLE, puede eliminar de forma segura las entradas correspondientes de la tabla CHANGE_CAUSE_TABLE.

Para liberar espacio de almacenamiento en las bases de datos de TADDM, utilice las consultas SQL para eliminar manualmente los datos antiguos de la tabla CHANGE_HISTORY_TABLE. El mandato siguiente es un ejemplo de dicho tipo de consulta SQL, en la que el entero 1225515600000 representa la fecha, 1 de

noviembre de 2008, expresada en el mismo formato que la devuelta por el método Java System.currentTimeMillis(), o un número igual a la diferencia, medido en milisegundos, entre la hora actual y la medianoche, 1 de enero de 1970 UTC:

```
DELETE FROM CHANGE_HISTORY_TABLE
WHERE PERSIST_TIME < 1225515600000 (ésta es la
indicación de fecha y hora Java)
```

Para convertir una fecha en una indicación de fecha y hora Java, utilice el código siguiente:

```
import java.util.*;
import java.text.*;
import java.sql.Timestamp;

public class DateToString {

  public static void main(String args[]) {
  try {
     String str = args[0];
     SimpleDateFormat formatter = new SimpleDateFormat("dd/MM/yyyy");
     Date date = formatter.parse(str);

    long msec = date.getTime();

    System.out.println("Date is " +date);
    System.out.println("MillSeconds is " +msec);

    } catch (ParseException e)
    {System.out.println("Exception :"+e);  }

  }
}
```

Ejecute el código tal como se indica a continuación:

```
java DateToString 1/11/2008
La fecha es Sáb 1 de nov 00:00:00 EST 2008
Los milisegundos son 1225515600000
```

Utilice la indicación de fecha y hora Java resultante en la consulta SQL.

Si existe una cantidad de registros excepcional en la tabla CHANGE_HISTORY_TABLE, pueden ser necesarias supresiones incrementales (supresión de un subconjunto de registros simultáneamente) para evitar rellenar registros de transacciones en la base de datos.

Después de eliminar la tabla CHANGE_HISTORY_TABLE, puede eliminar de forma segura las entradas correspondientes de la tabla CHANGE_CAUSE_TABLE. CHANGE_CAUSE_TABLE es una tabla de enlace que se utiliza para propagar los cambios. Por ejemplo, si añade un nuevo componente de software al sistema operativo, la tabla vincula este cambio al equipo en el que se ejecuta el sistema operativo. Para eliminar registros de la tabla CHANGE_CAUSE_TABLE, utilice el siguiente comando:

```
delete from change_cause_table where cause_id not in (select id from change_history_table)
```

Marcos temporales para eliminar datos

Para limitar el crecimiento de la base de datos con el tiempo, puede gestionar el tamaño de los datos del historial almacenados en TADDM. Cuando determine el marco temporal óptimo para eliminar datos de la tabla del historial de cambios, tenga en cuenta el uso que hace de los datos del historial y si la información de estos la utilizan también otras aplicaciones.

Si hay otras aplicaciones que utilizan la información de los datos del historial, asegúrese de efectuar las sincronizaciones más frecuentemente que el número de semanas de mantenimiento de los datos del historial de cambios en la tabla CHANGE_HISTORY_TABLE.

Los siguientes ejemplos muestran algunos escenarios típicos:

- Si utiliza datos del historial de cambios para la determinación de problemas y desea investigar problemas que se produjeron hace cinco semanas, mantenga como mínimo cinco semanas de datos en la tabla CHANGE_HISTORY_TABLE.
- Si sincroniza Tivoli Business Service Manager (TBSM) semanalmente, mantenga más de una semana de datos del historial de cambios en la tabla del historial de cambios de TADDM.

Es importante tener en cuenta que en los despliegues del servidor de sincronización, si hay una gran cantidad de datos del historial de cambios en los servidores del dominio, aumenta el tiempo que tarda en completarse una sincronización completa.

Mantenimiento de datos en un despliegue de servidor de sincronización

En un despliegue de servidor del dominio, puede basar las decisiones de mantenimiento de datos solamente en las necesidades de datos del dominio. Sin embargo, en un despliegue de servidor de sincronización, debe coordinar la eliminación de datos del historial de cambios entre cada base de datos del servidor del dominio y la base de datos del servidor de sincronización, y debe eliminar los datos de todas las bases de datos.

En un despliegue de servidor de sincronización, utilice las siguientes directrices para el mantenimiento de datos:

- Mantenga los datos del historial de cambios en un nivel de dominio durante un periodo de tiempo que sea superior al periodo de tiempo entre las sincronizaciones planificadas de cada base de datos del servidor del dominio con la base de datos del servidor de sincronización. Por ejemplo, si la sincronización se produce semanalmente, mantenga como mínimo dos semanas de datos del historial de cambios en cada base de datos del servidor del dominio.
- Elimine primero los datos de la base de datos del servidor del dominio. A continuación, elimine los datos de la base de datos del servidor de sincronización.
- La práctica recomendada es mantener el mismo número de semanas de datos del historial de cambios en todas las bases de datos de TADDM. Sin embargo, el período de conservación de los datos del historial de cambios en la base de datos del servidor de sincronización puede variar del período que estos datos se mantienen en las bases de datos del servidor del dominio.
- Después de que haya determinado un marco temporal para la eliminación de datos que satisfaga las necesidades específicas del entorno, es recomendable eliminar los datos justo después de que se produzca una sincronización entre las bases de datos del servidor del dominio y la base de datos del servidor de sincronización.

Supresión de registros de la tabla ALIASES_JN:

Si se suprimen registros antiguos de la tabla ALIASES_JN, se puede mejorar el rendimiento y la usabilidad de la herramienta de integridad de datos y es posible liberar espacio adicional en la base de datos.

Acerca de esta tarea

La tabla ALIASES_JN incluye el historial de los cambios en la tabla ALIASES. La herramienta de integridad de los datos requiere los datos recopilados para encontrar posibles sobrefusiones de elementos de configuración en la base de datos. A lo largo del tiempo, el número de registros de la tabla ALIASES_JN alcanza un tamaño considerable. El tamaño de esta tabla afecta al rendimiento y a la usabilidad de la herramienta de integridad de los datos y aumenta la necesidad de espacio de almacenamiento en la base de datos TADDM.

El agente de topología `AliasesJnTableCleanup` realiza la limpieza de la tabla ALIASES_JN.

De forma predeterminada, elimina todas las filas que tengan más de 30 días. Es posible cambiar con qué tiempo se suprimen los registros mediante la configuración de la siguiente propiedad en el archivo `collation.properties`:

```
com.ibm.cdb.topomgr.topobuilder.agents.AliasesJnTableCleanupAgent.removeOlderThanDays=30
```

Si se define la propiedad con un valor de -1, el agente se inhabilita. Si el valor del tiempo se define demasiado bajo, la herramienta de verificación de datos con la opción de sobrefusión podría no producir resultados completos.

De forma predeterminada, el agente se ejecuta durante un máximo de 1800 segundos (30 minutos). Si este periodo de tiempo no es suficiente para eliminar todas las filas viejas, se realiza un intento por suprimir las restantes la siguiente vez que se ejecuta el agente. Es posible definir el valor de tiempo de espera del agente mediante la configuración de la siguiente propiedad en el archivo `collation.properties`:

```
com.ibm.cdb.topomgr.topobuilder.agents.AliasesJnTableCleanupAgent.timeout=1800
```

Mantenimiento de la base de datos DB2

Tiene que mantener la base de datos TADDM DB2 de forma regular para garantizar un rendimiento aceptable.

Acerca de esta tarea

Están disponibles las siguientes utilidades de DB2:

REORG

Tras haber efectuado muchos cambios en los datos de las tablas, provocados por la inserción, supresión y actualización de columnas de longitud variable, es posible que los datos secuenciales lógicamente se encuentren en páginas de datos físicos no secuenciales. Como consecuencia, el gestor de bases de datos realiza operaciones de lectura adicionales para acceder a los datos. Reorganice las tablas de DB2 para eliminar la fragmentación y recuperar espacio mediante el programa de utilidad **REORG**. Utilice la utilidad **REORG** según sea necesario, si **RUNSTATS** tarda más de lo habitual en terminar o si el mandato **REORGCHK** de DB2 indica que es necesario. Cierre el servidor TADDM cuando ejecute la utilidad **REORG**, ya que durante una reorganización de tablas o índices fuera de línea (refragmentación de datos), las aplicaciones puede acceder a los datos de las tablas, pero no actualizarlos. Como TopologyBuilder se ejecuta a menudo, incluso sin descubrimiento, esos bloqueos puedes provocar resultados impredecibles en la aplicación.

RUNSTATS (recopilación de estadísticas manuales)

El optimizador de DB2 utiliza información y estadísticas del catálogo de

DB2 para determinar el mejor acceso a la base de datos, que se basa en la consulta que se proporciona. La información sobre estadísticas se recopila para las tablas e índices específicos de la base de datos local, cuando se ejecuta el programa de utilidad **RUNSTATS**. Cuando añada o elimine un número significativo de filas de tabla, o si actualiza los datos de las columnas para las que se recopila información de estadísticas, utilice el mandato **RUNSTATS** para actualizar las estadísticas. Para obtener un rendimiento óptimo, complete las tareas **RUNSTATS** semanal o diariamente si la actividad de la base de datos es muy elevada. La falta de estadísticas actualizadas puede provocar una degradación grave del rendimiento de TADDM. Puede ejecutar la utilidad **RUNSTATS** mientras se está ejecutando el servidor TADDM. TADDM requiere un formato **RUNSTATS** específico que se describe más adelante. La opción **AUTO_RUNSTATS** de DB2 tiene que estar desactivada.

AUTO_RUNSTATS (recopilación de estadísticas automáticas)
Habilite la recopilación automática de estadísticas, también conocida como **auto-runstats**, para que DB2 decida si es necesario actualizar las estadísticas de la base de datos de TADDM. El programa de utilidad **RUNSTATS** se ejecuta en un segundo plano y las estadísticas de la base de datos se mantienen siempre actualizadas.

Para habilitar la recopilación de estadísticas automáticas, debe establecer los parámetros AUTO_MAINT, AUTO_TBL_MAINT y AUTO_RUNSTATS en ON. Ejecute el comando siguiente:

```
CONNECT TO <alias db>
UPDATE DB CONFIG USING AUTO_MAINT ON AUTO_TBL_MAINT ON AUTO_RUNSTATS ON
```

donde <*alias db*> es el nombre de la base de datos.

Restricción: Este programa de utilidad únicamente se puede utilizar si el DB2 APAR IT05733 está instalado y si se ha establecido el parámetro DB2_SELECTIVITY=DSCC. El DB2 APAR IT05733 se incluye en los siguientes y posteriores releases de DB2:

- 9.7 Fix Pack 11
- 10.1 Fix Pack 6
- 10.5 Fix Pack 7

Para establecer el parámetro DB2_SELECTIVITY=DSCC en DB2 versión 10.*x*, ejecute el siguiente mandato:

```
db2set -immediate DB2_SELECTIVITY=DSCC
```

Nota: DB2 9.7 no da soporte al parámetro -immediate. Para establecer el parámetro DB2_SELECTIVITY=DSCC en esta versión, ejecute el mandato **db2set DB2_SELECTIVITY=DSCC** y reinicie DB2.

Nota: Si el usuario de TADDM actualiza la versión de DB2 en una instalación de TADDM, también debe actualizarse la versión compatible del controlador. Puede pedir el DBA para db2jcc.jar del servidor DB2 de TADDM, o puede descargar el adecuado para su versión de DB2 aquí: http://www-01.ibm.com/support/docview.wss?uid=swg21363866. Cuando lo tenga, pare TADDM, cópielo a dist/lib/jdbc/, confirme que los permisos son correctos para que el usuario de TADDM pueda leer el archivo e inicie TADDM. Repita este paso en todos los servidores TADDM de su entorno.

DB2 HEALTH MONITOR

Es aconsejable ejecutar el supervisor de estado de DB2 en la base de datos TADDM para supervisar si se modifican condiciones como **RUNSTATS**, o **REORG**, o si hace falta algún ajuste. El supervisor de estado puede avisar al administrador de base de datos de problemas potenciales de salud del sistema. El supervisor de estado detecta problemas que pueden conducir a fallos de hardware o a un rendimiento o capacidad inaceptable del sistema. Gracias a esta supervisión de estado, puede hacer frente a un problema antes de que afecte realmente al rendimiento del sistema.

DB2 PERFORMANCE ANALYSIS SUITE

Cuando se sospecha que puede existir un problema en DB2, la herramienta Performance Analyst analiza una instantánea de DB2 que se toma durante el fallo y se sugieres acciones. Puede descargar esta herramienta en https://www.ibm.com/developerworks/community/groups/community/perfanalyst.

Para tomar una instantánea DB2 de TADDM,siga los pasos siguientes:

1. Conecte su base de datos TADDM desde el servidor DB2 y ejecute el mandato siguiente:

   ```
   db2 -tf updmon.sql
   ```

   en el que el archivo `updmon.sql` incluye las siguientes entradas:

   ```
   UPDATE MONITOR SWITCHES USING BUFFERPOOL ON ;
   UPDATE MONITOR SWITCHES USING LOCK       ON ;
   UPDATE MONITOR SWITCHES USING SORT       ON ;
   UPDATE MONITOR SWITCHES USING STATEMENT  ON ;
   UPDATE MONITOR SWITCHES USING TABLE      ON ;
   UPDATE MONITOR SWITCHES USING UOW        ON ;
   UPDATE MONITOR SWITCHES USING TIMESTAMP  ON ;
   RESET MONITOR ALL
   ```

2. Una vez completado el paso 1, ejecute el mandato “DB2 get monitor switches” para comprobar que todo esté definido. Todos tienen que tener el estado `ON`.
3. Ejecute el proceso con el que ha experimentado problemas.
4. En intervalos adecuados, mientras se ejecuta el proceso lento, ejecute el siguiente mandato desde DB2:

   ```
   db2 get snapshot for all on <dbname> > <dbname>-dbsnap.out
   ```

   Ejecute este mandato desde la misma ventana desde la que ejecutó el mandato del paso 1. Este mandato no se puede ejecutar sin utilizar el script.
5. Ejecute las instantáneas utilizando un archivo de salida de fecha y hora diferente cada vez. Ejecútelo a intervalos de forma que consiga tres o cuatro instantáneas durante el proceso, pero que el tiempo entre ejecuciones no supere la hora.

Una vez recogidas las instantáneas, analícelas con la herramienta Performance Analyst, comenzando por la última instantánea. Por ejemplo, una alta ocupación de la CPU o un tiempo de ejecución más alto de lo habitual en la pestaña Sentencia para una consulta que se ejecuta varias veces suele indicar un problema de optimización, que puede resolverse con la utilidad **RUNSTATS**. Un porcentaje de desbordamiento elevado en la pestaña tablas puede indicar la necesidad de utilizar la utilidad **REORG**. Compruebe la pestaña agrupación de almacenamiento intermedio para asegurarse de que no hay alertas, una agrupación de almacenamiento intermedio demasiado pequeña puede provocar un rendimiento bajo.

Antes de empezar

Después de cualquier mantenimiento importante que genere un cambio de esquema, por ejemplo, tras aplicar un fixpack, debe generar el archivo `TADDM_table_statistics.sql` en el servidor de almacenamiento de TADDM. El archivo es necesario para una de las tareas de mantenimiento de la base de datos **RUNSTATS** que debe realizarse de forme regular. TADDM necesita un formato especial para actualizar estadísticas de la base de datos a causa de una limitación de DB2 al gestionar columnas con prefijos comunes largos como los nombres de clase, que se utilizan de forma común en TADDM. Por este motivo, no utilice la opción **AUTO_RUNSTATS** de DB2, utilice la sintaxis **RUNSTATS** que genere al completar los siguientes pasos. Sin embargo, si tiene instalado el DB2 APAR IT05733 y ha establecido el parámetro `DB2_SELECTIVITY=DSCC`, puede utilizar la opción **AUTO_RUNSTATS**.

Nota: Las siguientes instrucciones se proporcionan para los sistemas operativos Linux y UNIX. Para realizar el mantenimiento de bases de datos en el sistema operativo Windows, utilice el script `.bat` correspondiente en lugar del script `.sh`.

Para generar el archivo `TADDM_table_stats.sql`, complete los siguientes pasos:

1. Ejecute el comando siguiente:
   ```
   cd $COLLATION_HOME/bin
   ```
2. Ejecute el siguiente mandato, donde *tmpdir* es un directorio en el que puede crearse este archivo:
   ```
   ./gen_db_stats.jy > tmpdir/TADDM_table_stats.sql
   ```
   En un despliegue de servidor de modalidad continua, ejecute este mandato en el servidor de almacenamiento primario.
3. Copie el archivo en la base de datos del servidor, o proporcióneselo al administrador de la base de datos (DBA) para ejecutarlo en la base de datos TADDM como se muestra en step 2 en el Procedimiento. Actualice las estadísticas de la base de datos al menos una vez a la semana o con más frecuencia si hay cambios importantes en alguna de las tablas.

Procedimiento

Para realizar el mantenimiento en una base de datos DB2, complete los siguientes pasos:

1. Para utilizar el programa de utilidad **REORG**, complete los siguientes pasos:
   a. En el servidor de la base de datos, coloque la siguiente consulta SQL, que genera los mandatos **REORG TABLE**, en un archivo:
   ```
   select 'reorg table '||CAST(RTRIM(creator) AS VARCHAR(40))||'.
    "'||substr(name,1,60)||'" ; ' from sysibm.systables where creator
    = 'UsuarioBD' and type = 'T' and name not in ('CHANGE_SEQ_ID')
    order by 1;
   ```
   donde *usuario_BD* es el valor de `com.collation.db.user=`.

   Nota: Asegúrese de que las mayúsculas y minúsculas de *dbuser* sean iguales que las del valor especificado en la tabla `sysibm.systables` de la base de datos, en la columna `creator`.
   b. Detenga el servidor de TADDM.

c. En una línea de mandatos de DB2, conéctese a la base de datos y ejecute los mandatos siguientes:

```
db2 –x –tf temp.sql > cmdbreorg.sql
db2 –tvf cmdbreorg.sql > cmdbreorg.out
```

d. Asegúrese de que la utilidad **REORG** sea correcta comprobando que no hay errores en el archivo `cmdbreorg.out`.

e. Inicie el servidor de TADDM.

2. Para utilizar el programa de utilidad **RUNSTATS**, complete los siguientes pasos. Automatice el proceso para que se ejecute al menos una vez a la semana.

a. En el servidor de bases de datos, ejecute el mandato **RUNSTATS** de TADDM utilizando la salida que ha generado antes:

```
db2 -tvf tmpdir/TADDM_table_stats.sql  > table_stats.out
```

b. Asegúrese de que la utilidad **RUNSTATS** sea correcta comprobando que no hay errores en el archivo `table_stats.out`.

Mantenimiento de bases de datos DB2 for z/OS

Estas directrices de aplicar y ajuste se aplican a las bases de datos IBM DB2 for z/OS.

Procedimiento

Estas directrices asumen que el *USUARIO_BD* es el ID de usuario primario de la base de datos DB2 y *USUARIO_ARCHIVADO* es el ID de usuario secundario de la base de datos DB2.

1. Utilice la consola de Discovery Management para ejecutar un descubrimiento. Este método llena la base de datos con los datos.
2. Detenga el servidor de TADDM.
3. Genere y ejecute la sentencia de control RUNSTATS para cada espacio de tabla utilizado por TADDM.

```
SELECT 'REORG TABLESPACE '||DBNAME||'.'||NAME FROM SYSIBM.SYSTABLESPACE
 WHERE CREATOR IN ('USUARIO_DB', 'USUARIO_ARCHIVADO') ORDER BY 1;
```

4. Genere y ejecute la sentencia de control RUNSTATS para los índices utilizados por TADDM.

```
SELECT 'REORG INDEX '||CREATOR||'.'||NAME FROM SYSIBM.SYSINDEXES
 WHERE CREATOR IN ('USUARIO_DB', 'USUARIO_ARCHIVADO');
```

5. Genere y ejecute la sentencia de control RUNSTATS para los espacios de tabla utilizados por TADDM.

```
SELECT 'RUNSTATS TABLESPACE '||DBNAME||'.'||NAME||' INDEX(ALL)
SHRLEVEL REFERENCE' FROM SYSIBM.SYSTABLESPACE
WHERE CREATOR IN ('USUARIO_DB', 'USUARIO_ARCHIVADO') ORDER BY 1;
```

6. Regenere y ejecute las sentencias de estadísticas de índice de UPDATE para cada usuario de base de datos de TADDM.

```
SELECT 'UPDATE SYSIBM.SYSINDEXES SET FIRSTKEYCARDF=FULLKEYCARDF
WHERE NAME = '||''''||CAST(RTRIM(name) AS VARCHAR(40))||''''||'
AND CREATOR = '||''''||CAST(RTRIM(creator) AS VARCHAR(40))||''''||'
AND TBNAME = '||''''||CAST(RTRIM(tbname) AS VARCHAR(40))||''''||'
AND TBCREATOR = '||''''||CAST(RTRIM(tbcreator) AS VARCHAR(40))||''''||';'
from sysibm.sysindexes a
where tbcreator in ('USUARIO_DB', 'USUARIO_ARCHIVADO');
AND  NAME IN
(SELECT IXNAME
FROM SYSIBM.SYSKEYS B
WHERE A.CREATOR = B.IXCREATOR
AND A.NAME    = B.IXNAME
AND COLNAME = 'PK__JDOIDX')
```

```
AND TBNAME IN
(SELECT NAME
FROM SYSIBM.SYSTABLES C
WHERE A.TBCREATOR = C.CREATOR
AND A.TBNAME = C.NAME
AND CARDF > 0);
```

donde USUARIO_BD es el ID de usuario primario de la base de datos DB2 y USUARIO_ARCHIVADO es el ID de usuario secundario de la base de datos de DB2.

7. Regenere y ejecute las sentencias de estadísticas de columna de UPDATE para cada usuario de base de datos de TADDM.

```
SELECT 'UPDATE SYSIBM.SYSCOLUMNS SET COLCARDF=(SELECT FULLKEYCARDF FROM
SYSIBM.SYSINDEXES WHERE NAME = '||''''||CAST(RTRIM(name)
AS VARCHAR(40))||''''||'
AND CREATOR = '||''''||CAST(RTRIM(creator) AS VARCHAR(40))||''''||'
AND TBNAME = '||''''||CAST(RTRIM(tbname) AS VARCHAR(40))||''''||'
AND TBCREATOR = '||''''||CAST(RTRIM(tbcreator) AS VARCHAR(40))||''''||')
WHERE NAME = '||''''||'PK__JDOIDX'||''''||' AND TBNAME = '||''''||
CAST(RTRIM(tbname) AS VARCHAR(40))||''''||'
AND TBCREATOR = '||''''||CAST(RTRIM(tbcreator) AS VARCHAR(40))||''''||';'
from sysibm.sysindexes a
where tbcreator in ('USUARIO_DB', 'USUARIO_ARCHIVADO');
AND  NAME IN
(SELECT IXNAME
FROM SYSIBM.SYSKEYS B
WHERE A.CREATOR = B.IXCREATOR
AND A.NAME    = B.IXNAME
AND COLNAME = 'PK__JDOIDX')
AND TBNAME IN
(SELECT NAME
FROM SYSIBM.SYSTABLES C
WHERE A.TBCREATOR = C.CREATOR
AND A.TBNAME = C.NAME
AND CARDF > 0);
```

8. Supervise regularmente las tablas más grandes en base a su uso de TADDM y ajuste sus atributos de almacenamiento si es necesario. En concreto, supervise el tamaño de las siguientes tablas de base de datos, que pueden llegar a ser muy grandes:
   - ALIASES
   - CHANGE_CAUSE_TABLE
   - CHANGE_HISTORY_TABLE
   - MSSOBJLINK_REL
   - PERSOBJ
   - SUPERIORS

   Utilice las sentencias ALTER para modificar los atributos *CANTPRI* y *CANTSEC*, en función de las necesidades de su entorno. Si resulta adecuado, considere la posibilidad de mover las tablas a espacios de tabla separados.
9. Utilice el mandato REBIND en los paquetes siguientes, con la opción KEEPDYNAMIC(YES):
   - SYSLH200
   - SYSLH201
   - SYSLH202

Mantenimiento de bases de datos Oracle

Estas directrices de mantenimiento y ajuste se aplican a las bases de datos Oracle.

1. Ejecute el paquete dbms_stats en las tablas de la base de datos. Oracle utiliza un optimizador basado en costes. El optimizador basado en costes necesita los datos para poder decidir sobre el plan de acceso y estos datos se generan

mediante el paquete dbms_stats. Las bases de datos Oracle dependen de los datos relativos a las tablas y los índices. Sin ellos, el optimizador tiene que realizar una estimación.

Volver a crear los índices y a ejecutar el paquete dbms_stats, resulta esencial para poder obtener un rendimiento óptimo con las bases de datos Oracle. Una vez llenada la base de datos, esta acción debe llevarse a cabo de forma planificada y periódica, por ejemplo, semanalmente.

- **REBUILD INDEX**: tras haber efectuado muchos cambios en los datos de las tablas, provocados por la inserción, supresión y actualización de la actividad, es posible que los datos secuenciales lógicamente se encuentren en páginas de datos físicos no secuenciales, de forma que el gestor de base de datos debe llevar a cabo operaciones de lectura adicionales para poder acceder a los datos. Vuelva a crear los índices para mejorar el rendimiento del SQL.
  a. Genere los mandatos **REBUILD INDEX** ejecutando la sentencia de SQL siguiente en la base de datos Oracle, donde *usuarioBD* es el valor de `com.collation.db.user=`:

     ```
     select 'alter index UsuarioBD.'||index_name||' rebuild tablespace '
     ||tablespace_name||';' from dba_indexes where owner = 'usuarioBD'
     and index_type not in ('LOB');
     ```

     Esta acción genera todos los mandatos **ALTER INDEX** que necesita ejecutar.
  b. Ejecute los mandatos en SQLPLUS, o en un recurso parecido. Es posible que, para volver a crear los índices de una base de datos grande, se necesiten entre 15 y 20 minutos.

2. **DBMS_STATS**: utilice RDBMS de Oracle para recopilar muchos tipos diferentes de estadísticas, para poder mejorar aún más el rendimiento. El optimizador utiliza la información y las estadísticas del diccionario para determinar el mejor acceso a la base de datos, en función de la consulta que se proporcione. La información sobre estadísticas se recopila para las tablas e índices específicos de la base de datos local, cuando se ejecuta el mandato **DBMS_STATS**. Cuando añada o elimine un número significativo de filas de tabla, o si actualiza los datos de las columnas para las que se recopila información de estadísticas, vuelva a ejecutar el mandato **DBMS_STATS** para actualizar las estadísticas.
   - El programa `gen_db_stats.jy` del directorio `$COLLATION_HOME/bin` genera una salida de mandatos de la base de datos para que tanto la base de datos Oracle como la base de datos DB2 actualicen las estadísticas en las tablas de TADDM. En el ejemplo siguiente se muestra cómo se utiliza el programa:
     a. cd `$COLLATION_HOME/bin`
     b. Ejecute esta sentencia SQL, donde *DirTemp* es un directorio en el que se crea este archivo:

        ```
        ./gen_db_stats.jy > DirTemp/TADDM_table_stats.sql
        ```

        En un despliegue de servidor de modalidad continua, ejecute esta sentencia en el servidor de almacenamiento primario.
     c. Una vez completada esta acción, copie el archivo en el servidor de base de datos y ejecute el mandato siguiente:
        – Para ejecutar un archivo de script en SQLPlus, escriba @ y, a continuación, el nombre del archivo: `SQL > @{file}`
     d. Ejecute los mandatos en SQLPLUS, o en un recurso parecido.

3. Agrupación de almacenamiento intermedio: una agrupación de almacenamiento intermedio o una memoria caché de almacenamiento intermedio es una estructura de memoria dentro del área global del sistema Oracle (SGA) para cada instancia. Esta memoria caché de almacenamiento intermedio se utiliza para colocar los bloques de datos en la memoria caché de la memoria. Acceder

a los datos de la memoria es mucho más rápido que acceder a ellos desde el disco. El objetivo del ajuste del almacenamiento intermedio de bloque es colocar en la memoria caché, de forma eficaz, los datos de bloques que se utilizan con frecuencia en la memoria caché de almacenamiento intermedio (SGA), y proporcionar un acceso más rápido a los datos. El ajuste del almacenamiento intermedio de bloque es una tarea clave en cualquier iniciativa de ajuste de Oracle, y forma parte del ajuste y la supervisión continuos de las bases de datos de producción. El producto Oracle mantiene su propia memoria caché de almacenamiento intermedio dentro de la SGA para cada instancia. Una memoria caché de almacenamiento intermedio con el tamaño adecuado puede obtener, normalmente, un índice de acceso de memoria caché superior al 90%, los que significa que nueve de cada diez solicitudes se gestionan sin acceder al disco. Si una memoria caché de almacenamiento intermedio es demasiado pequeña, el índice de acceso de memoria caché será demasiado pequeño, y dará como resultado que se generen más operaciones de E/S de disco físico. Si una memoria caché de almacenamiento intermedio es demasiado grande, las partes de la memoria caché de almacenamiento intermedio se infrautilizan, y se desperdician los recursos de la memoria.

Tabla 36. Directrices del tamaño de la agrupación de almacenamiento intermedio: (tamaño_caché_BD)

Número de elementos configurables	Directrices de tamaño de la agrupación de almacenamiento intermedio
< 500.000	38.000
500.000 - 1.000.000	60.000
> 1.000.000	95.000

4. Puede duplicar el tamaño máximo de cursores abiertos si el descubrimiento o la carga masiva tarda mucho tiempo en completarse y NRS contienen el error siguiente:

```
com.ibm.tivoli.namereconciliation.service.NrsService
getAliases(masterGuid)
GRAVE: NOTA ⌂*** Estado de SQL = 60000.   Código de SQL = 604.   Mensaje de SQL =
ORA-00604: se ha producido un error en el nivel 1 de SQL recursivo.
ORA-01000: se ha superado el número máximo de cursores abiertos.
ORA-01000: se ha superado el número máximo de cursores abiertos.
```

5. Verifique que las versiones del controlador Oracle JDBC y del servidor Oracle son iguales. Si es necesario, sustituya el archivo del controlador JDBC de Oracle en las siguientes ubicaciones.

   Nota: Esto sólo se aplica cuando BIRT Report Viewer está habilitado.

   - TADDM 7.3.0 - `$COLLATION_HOME/deploy-tomcat/birt-viewer/WEB-INF/platform/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers/`
   - TADDM 7.3.0.1 y posterior: `$COLLATION_HOME/apps/birt-viewer/WEB-INF/platform/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers/`
   - `$COLLATION_HOME/lib/jdbc/`

Comunicación de base de datos

Cuando la base de datos no está disponible, el servidor de almacenamiento intenta establecer la conexión de nuevo.

Cuando no hay ninguna conexión entre la base de datos y el servidor de almacenamiento, el servidor de almacenamiento espera el tiempo especificado en la

propiedad com.ibm.cdb.db.timeout y realiza un intento de conexión a la base de datos. El número de reintentos para establecer la conexión está especificado en la propiedad com.ibm.cdb.db.max.retries.

Para obtener más información sobre las propiedades de la base de datos, vaya a la sección Propiedades de la base de datos.

Ajuste de rendimiento de descubrimiento

Puede actualizar las propiedades com.collation.discover.dwcount, com.collation.discover.observer.topopumpcount y com.ibm.cdb.discover.observer.topopump.threshold en el archivo collation.properties para influir en la tasa de descubrimiento y la velocidad a la que los resultados de descubrimiento se almacenan en la base de datos de TADDM o para limitar el número de hebras que son responsables de almacenar datos.

Para obtener detalles sobre estas propiedades, consulte "Propiedades de rendimiento" en la página 94.

Si aumenta los valores de las propiedades com.collation.discover.dwcount o com.collation.discover.observer.topopumpcount, puede que también tenga que aumentar la memoria instalada aumentando el valor del tamaño de almacenamiento dinámico máximo de las siguientes máquinas virtuales Java (JVM):

Para la propiedad dwcount:

- En un despliegue de servidor en modalidad continua:
  - Descubrir
  - DiscoverService
- En un despliegue de servidor de dominio:
  - Descubrir

Para la propiedad topopumpcount:

- En un despliegue de servidor en modalidad continua:
  - StorageService
- En un despliegue de servidor de dominio:
  - Topología

Para obtener más información, consulte "Máquina virtual Java Virtual Machine: ajuste de parámetros de IBM" en la página 155.

Para obtener más información sobre cómo ajustar el rendimiento del descubrimiento, consulte el documento titulado *Tuning Discovery Performance* en http://www.ibm.com/software/brandcatalog/ismlibrary/.

Ajuste del tipo de descubrimiento

El atributo del tipo de descubrimiento es el área con el mayor potencial para el ajuste. La propiedad con mayor impacto sobre el rendimiento es el número de hebras Worker de descubrimiento. También puede utilizar los sensores en curso para supervisar el rendimiento o mejorarlo especificando los tamaños de agrupación de sesiones.

Una hebra Worker de descubrimiento es una hebra que ejecuta sensores. La propiedad siguiente especifica el número máximo de hebras Worker de descubrimiento:

```
com.collation.discover.dwcount=32
```

Si el servidor tiene suficiente capacidad libre, puede aumentar este número y permitir que más sensores se ejecuten en paralelo.

Sensores en curso

Para supervisar el rendimiento, puede revisar los sensores en curso. Un sensor en curso se puede encontrar en una de estas tres fases de la ejecución:

started
: Un sensor en esta fase está descubriendo uno o varios elementos de configuración.

discovered
: Un sensor en esta fase ha terminado de descubrir uno o varios elementos de configuración, pero está esperando a que sus resultados se guarden en el almacén de datos.

storing
: Un sensor en esta fase guarda los resultados del descubrimiento en la base de datos.

Para ordenar los sensores en curso por fase de ejecución, pulse la columna Descripción.

Al observar la ejecución de un descubrimiento y comparar el número de sensores en curso que se encuentran en la fase de inicio (started) con el número de sensores en curso en las fases de descubrimiento (discovered) o almacenaje (storing), puede evaluar si el descubrimiento de atributos es más rápido o más lento que el almacenamiento de atributos de un entorno en concreto. Al igual que con todos los cambios realizados sobre el archivo `collation.properties`, debe reiniciar el servidor para que el cambio entre en vigor.

Ejemplos:

Sensores en curso: STARTED, DISCOVERED, STORING.

Si el número de (DISCOVERED + STORING) es inferior al de STARTED, podría indicar que el descubrimiento es el cuello de botella de rendimiento.

Si el número de (DISCOVERED + STORING) supera al de STARTED, podría indicar que el almacenamiento es el cuello de botella de rendimiento.

Tamaños de agrupación de sesión y pasarela

Para descubrir los atributos de un elemento de configuración en concreto, un sensor requiere una sesión de SSH o WMI con su sistema principal. Para mejorar el rendimiento, estas sesiones se agrupan y se almacenan en memoria caché. Los tamaños de agrupación predeterminados resultan suficientes la mayoría de las veces, pero si no son lo bastante grandes, pueden limitar el tipo de descubrimiento. Puede cambiar la siguiente propiedad a `true` para supervisar esta condición:

```
com.collation.platform.session.ExtraDebugging=false
```

Debe reiniciar el servidor de descubrimiento para que el cambio entre en vigor. Una vez ejecutado un descubrimiento, puede buscar en los registros de DiscoverManager problemas derivados del tiempo de espera relacionados con las

agrupaciones de sesión. Para ello, busque en los registros `pool lock`. A continuación, se muestra un ejemplo de la degradación del rendimiento debida a la contención de agrupaciones de sesiones:

```
2006-08-04 16:11:50,733 DiscoverManager [DiscoverWorker-34]
WindowsComputerSystemAgent(192.168.16.181)
INFO session.SessionClientPool -
Session client [3x ssh2:/admlxz@151.179.84.85]#9612508
waited 158.682 seconds for pool lock
```

Puede incrementar el tamaño de la agrupación si el tiempo de espera de una sesión es demasiado. Hay dos formas de hacerlo. Puede cambiar globalmente el tamaño de la agrupación para las sesiones de un host si edita la propiedad siguiente del archivo `collation.properties`:

```
com.collation.platform.session.PoolSize=3
```

Sin embargo, es poco probable que la contención se refiera a las sesiones de todos los hosts del entorno, o de la mayoría de ellos. Es posible que la contención esté restringida a un pequeño número de hosts más grandes que utilizan muchos sensores. El servidor de descubrimiento utiliza una propiedad con ámbito, lo que implica que muchas de las propiedades del archivo `collation.properties` utilizan un valor para destinos generales y otro para destinos específicos. Puede ajustar esta propiedad añadiendo una dirección IP o un nombre de ámbito del servidor de descubrimiento, como en el ejemplo siguiente:

```
com.collation.platform.session.PoolSize.10.10.250.1=20
```

En este caso, el tamaño de la agrupación para 10.10.250.1 es 20, pero para los hosts restantes, es 3. Puede buscar en los mensajes de registro, como el de los registros de DiscoverManager, y determinar para qué hosts no es suficiente el tamaño predeterminado de la agrupación de sesiones, además de realizar los cambios que correspondan en el archivo `collation.properties`.

Un valor relacionado es el tamaño de la agrupación de pasarelas. Establece el número de sesiones permitidas entre el servidor de descubrimiento y la pasarela de Windows. Puede especificarlo con la propiedad siguiente:

```
com.collation.platform.session.GatewayPoolSize=10
```

Si el entorno consta básicamente de sistemas informáticos Windows, ajuste esta propiedad hacia arriba, de manera que sea igual al número de hebras Worker de descubrimiento.

Ajuste de almacenamiento

El almacenamiento es la segunda área principal que hay que ajustar. Si el número de sensores de la fase de almacenamiento equivale aproximadamente al valor de la propiedad que especifica el número de hebras de almacenamiento paralelas, el almacenamiento de los resultados del descubrimiento está provocando el cuello de botella de rendimiento. Para mejorar el rendimiento, también puede limitar el número de hebras que se encargan del almacenamiento de datos.

La siguiente propiedad especifica el número de hebras de almacenamiento paralelas. Se trata de uno de los valores principales para controlar el rendimiento del almacenamiento de descubrimiento:

```
com.collation.discover.observer.topopumpcount
```

Para mejorar el rendimiento del almacenamiento cuando los agentes de topología están en ejecución, puede limitar el número de hebras que son responsables del almacenamiento de datos durante un descubrimiento. Como resultado, el

descubrimiento tarda menos tiempo en completarse. Para especificar el límite de hebras que se ejecutan, edite las siguientes propiedades en el archivo `collation.properties`:

com.ibm.cdb.discover.observer.topopump.threshold
Esta propiedad especifica el número de hebras de almacenamiento que es el límite.

com.ibm.cdb.discover.observer.topopump.threshold.<nombre_grupo_agentes>
Esta propiedad especifica el número de hebras de almacenamiento que es el límite cuando se ejecute el grupo de agentes especificado.

La siguiente tabla en qué medida la propiedad `com.ibm.cdb.discover.observer.topopump.threshold` puede mejorar el rendimiento del descubrimiento. Los cálculos son respecto a una base de datos con 76 000 elementos de configuración.

Valor de propiedad de umbral	Mejora del tiempo en porcentaje
0,2	55
0,5	33
0,7	13
1	0

Máquina virtual Java Virtual Machine: ajuste de parámetros de IBM

Puede definir los parámetros de la máquina virtual Java(JVM) para reducir la fragmentación del almacenamiento dinámico de Java y ayudar a mejorar el rendimiento.

La fragmentación del almacenamiento dinámico Java se puede producir a medida que aumente el número de objetos que se procesen. Hay varios parámetros que puede establecer para ayudarle a reducir la fragmentación en el almacenamiento dinámico.

- Un kCluster es un área de almacenamiento que se utiliza exclusivamente para los bloques de clase. Es lo bastante grande como para poder contener 1280 entradas. Cada bloque de clase tiene una longitud de 256 bytes. Este valor predeterminado es, normalmente, demasiado pequeño, y puede provocar la fragmentación del almacenamiento dinámico. Establezca el parámetro del kCluster, **-Xk**, tal como se indica a continuación, para ayudarle a reducir la fragmentación del almacenamiento dinámico. Éstos son los valores iniciales, y es posible que deban ajustarse en su entorno. Efectuar un análisis de un volcado del almacenamiento dinámico es lo mejor que se puede hacer para determinar el tamaño ideal.
  - Topology: -Xk8300
  - EventsCore: -Xk3500
  - DiscoverAdmin: -Xk3200
  - Proxy: -Xk5700
  - Discover: -Xk3700

  Implemente estos valores en el archivo `collation.properties` añadiendo entradas a la sección de valores específicos del proveedor de la JVM. Por ejemplo, para implementar estos cambios para el servidor de topologías, añada la línea siguiente:

```
com.collation.Topology.jvmargs.ibm=-Xk8300
```

- Otra opción que sirve para resolver los problemas de fragmentación es asignar, específicamente, cierta cantidad de espacio para los objetos grandes; > 64K. Utilice el parámetro **-Xloratio**. Por ejemplo:

  – **-Xloratio0.2**

  Este mandato reserva el x% del almacenamiento dinámico Java activo (no el x% de -Xmx sino el x% del tamaño del almacenamiento dinámico Java actual), sólo para la asignación de objetos grandes (≥64 KB). Si se cambia, debe cambiarse -Xmx para garantizar que no se reduzca el tamaño del área de objetos pequeños. Efectuar un análisis de un volcado del almacenamiento dinámico es lo mejor que se puede hacer para determinar el valor ideal de este parámetro.

Hay algunos parámetros que se pueden establecer que afectan al rendimiento de Java. Para cambiar una opción de la JVM existente por un valor diferente, edite uno de los archivos siguientes:

- Para un servidor de dominio en TADDM 7.3.0, el archivo `$COLLATION_HOME/deploy-tomcat/ROOT/WEB-INF/cmdb-context.xml`.
- Para un servidor de dominio en TADDM 7.3.0.1 y posterior, el archivo `$COLLATION_HOME/apps/ROOT/WEB-INF/cmdb-context.xml`.
- Para un servidor de sincronización en TADDM 7.3.0, el archivo `$COLLATION_HOME/deploy-tomcat/ROOT/WEB-INF/ecmdb-context.xml`.
- Para un servidor de sincronización en TADDM 7.3.0.1 y posterior, el archivo `$COLLATION_HOME/apps/ROOT/WEB-INF/ecmdb-context.xml`.
- Para un servidor de detección en TADDM 7.3.0, el archivo `$COLLATION_HOME/deploy-tomcat/ROOT/WEB-INF/discovery-server-context.xml`.
- Para un servidor de detección en TADDM 7.3.0.1 y posterior, el archivo `$COLLATION_HOME/apps/ROOT/WEB-INF/discovery-server-context.xml`.
- Para un servidor de almacenamiento en TADDM 7.3.0, el archivo `$COLLATION_HOME/deploy-tomcat/ROOT/WEB-INF/storage-server-context.xml`.
- Para un servidor de almacenamiento en TADDM 7.3.0.1 y posterior, el archivo `$COLLATION_HOME/apps/ROOT/WEB-INF/storage-server-context.xml`.

Para editar uno de estos archivos con el fin de cambiar los valores de uno de los servicios de TADDM debe buscar, en primer lugar, el servicio en el archivo. A continuación, figura un ejemplo del principio de una definición de servicio incluida en el archivo XML:

```
<bean id="Discover"
 class="com.collation.platform.service.ServiceLifecycle" init-method="start"
 destroy-method="stop">
 <property name="serviceName">
  <value>Discover</value>
 </property>
```

Dentro de la definición existen ciertos elementos y atributos que controlan los argumentos de la JVM. Por ejemplo:

```
<property name="jvmArgs">
 <value>-Xms8M;-Xmx512M;
 -Djava.nio.channels.spi.SelectorProvider=sun.nio.ch.PollSelectorProvider
 </value>
</property>
```

Los argumentos de la JVM se pueden establecer como una lista separada por puntos y coma, en el elemento siguiente:

```
<property name="jvmArgs"><value>
```

También puede modificar las propiedades de la máquina virtual Java que están en el archivo `collation.properties`. Estas propiedades pueden tener una de las siguientes formas:

com.collation.JVM.jvmargs.PROVEEDOR
Dicha propiedad se añade a los valores que se leen desde el archivo `*-config.xml`.

com.collation.jvmargs.PROVEEDOR
Dicha propiedad se añade a todas las máquinas virtuales Java de TADDM.

com.collation.JVM.jvmargs
Dicha propiedad sobrescribe todos los valores que se especifican en el archivo `*-config.xml`.

donde

- `JVM` es `Proxy`, `Topology`, `EventsCore`, `ExcmdbCore`, `DiscoverAdmin`, `StorageService`, `DiscoveryService`.
- `VENDOR` es `ibm` o `sun`.

Ajuste de propiedades de Java Virtual Machine

En el archivo `collation.properties`, los valores predeterminados para las propiedades de máquina virtual Java Machine (JVM) que se aplican a la consola de Discovery Management de TADDM se basan en el número de equivalentes del servidor (SE) de su entorno.

Valores predeterminados para las propiedades de JVM que se aplican a la consola de Discovery Management

- Entorno pequeño (menos de 1000 SE):
  - com.collation.gui.initial.heap.size=128m
  - com.collation.gui.max.heap.size=512m
- Entorno mediano (1000–2500 SE):
  - com.collation.gui.initial.heap.size=256m
  - com.collation.gui.max.heap.size=768m
- Entorno grande (2500–5000 SE):
  - com.collation.gui.initial.heap.size=512m
  - com.collation.gui.max.heap.size=1024m

Ajuste de la red

Tras implementar un sistema, se debe supervisar la red para garantizar que no se consuma su ancho de banda por encima del 50%.

La red puede influir en el rendimiento global de la aplicación y normalmente se expone a sí misma como factor de rendimiento cuando hay un retraso en las situaciones siguientes:

- El retraso transcurrido entre el momento en que un sistema cliente envía una solicitud al servidor y el momento en que éste la recibe.
- El retraso transcurrido entre el momento en que el sistema servidor devuelve los datos al sistema cliente y éste los recibe.

Ajuste de DNS

TADDM es sensible al rendimiento de la infraestructura de DNS desplegada. Incluso si el rendimiento de DNS es adecuado para otras aplicaciones, puede ser necesaria cierta configuración para optimizar el rendimiento para TADDM.

TADDM realiza un gran número de consultas de búsqueda de DNS para resolver nombres de visualización significativos para componentes y sucesos. A diferencia de las mayoría de las demás aplicaciones, TADDM utiliza principalmente búsquedas inversas (correlación de direcciones IP con nombres) en lugar de búsquedas directas (correlación de nombres con direcciones IP).

Debido a este patrón de uso, los problemas con el rendimiento de DNS pueden tener un efecto mayor sobre el rendimiento de TADDM que en otras aplicaciones. Por ejemplo, un tiempo de respuesta de DNS de 500 milisegundos probablemente no afectaría de forma significativa a una aplicación típica, pero podría causar problemas perceptibles en TADDM, debido al gran número de consultas de DNS que lleva a cabo. Además, debido a que otras aplicaciones solo realizan la búsquedas directas, un problema de rendimiento en las búsquedas inversas no afectaría a la mayoría de las aplicaciones, pero sí que afectaría a TADDM.

En general, los problemas de rendimiento de la infraestructura de DNS se deben solventar para beneficiar a todos los consumidores de servicios de DNS. Si esto no es posible, existen varias formas en las que se puede mitigar el efecto de los problemas de rendimiento de DNS sobre TADDM:

- Asegúrese de que la delegación in-addr arpa para búsquedas inversas está configurada correctamente. Los problemas de delegación pueden provocar pausas o bloqueos largos durante las búsquedas inversas mientras el servidor de TADDM intenta conectar con servidores que no existen. Este tipo de problema de configuración solo afecta a aplicaciones (como, TADDM) que realizan búsquedas inversas.
- Configure al menos un servidor DNS de memoria caché/reenvío o un sistema de servidor TADDM, y configure los servidores TADDM que debe utilizar el servidor DNS para búsquedas. Esto permite que las búsquedas de DNS se almacenen en la memoria caché en el entorno de TADDM local en función de las reglas de vida de las zonas. Este tipo de servidor no tiene estado y, por lo tanto, requiere un mantenimiento mínimo y aumenta poco la sobrecarga.
- Configure al menos un servidor DNS esclavo o un sistema de servidor TADDM, y configure los servidores TADDM que debe utilizar el servidor DNS para búsquedas. Esto permite realizar búsquedas de DNS en el entorno de TADDM local sin comunicación con la infraestructura de DNS general. Un servidor DNS esclavo mantiene el estado de forma automática y, por lo tanto, requiere un mantenimiento mínimo y aumenta poco la sobrecarga.
- Utilice un método alternativo para búsquedas, como un archivo `hosts`, en vez de DNS. (Este método puede implicar grandes requisitos de mantenimiento).

Nota: No cambie los parámetros predeterminados de memoria caché de DNS en el archivo `java.security`. Aunque los parámetros de almacenamiento en memoria caché pueden afectar al rendimiento DNS, los cambios en este archivo de configuración no se conservan cuando se aplican arreglos de mantenimiento de TADDM. En su lugar, utilice uno de los métodos que se describen en esta sección para optimizar el rendimiento de DNS.

Ajuste del servidor de sincronización

El rendimiento del servidor de sincronización es altamente dependiente del procesamiento de la base de datos y, por lo tanto, del mantenimiento y ajuste de la base de datos. Si experimenta problemas de rendimiento con el procesamiento de sincronización, consulte la información del ajuste de la base de datos y observe los ajustes de la agrupación de almacenamiento intermedio para las bases de datos DB2, los ajustes del valor de memoria caché para las bases de datos Oracle y la información sobre el mantenimiento de la base de datos.

En concreto para el servidor de sincronización, actualice la configuración de la base de datos DB2 especificando el siguiente mandato:

```
UPDATE DATABASE CONFIG FOR TADDM USING
   UTIL_HEAP_SZ 5000
   LOGBUFSZ 1024
   LOCKLIST 20000
   SORTHEAP 2048
   PCKCACHESZ AUTOMATIC
;
```

Ajuste de sistema Windows

Para asignar más memoria a los servicios de TADDM, ajuste los sistemas Windows.

Complete las siguientes tareas:

- El archiva de paginación del sistema no debe estar ubicado en la misma unidad que el sistema operativo. Si fuera posible, coloque el archivo de paginación del sistema en una unidad de disco aparte.
- Configure el servidor de la base de datos y de la aplicación para que maximice los datos para las aplicaciones de red.

Informes

Puede crear y añadir informes personalizados al portal de gestión de datos mediante visores de informes externos, visores de informes de JSP o el sistema de informes BIRT.

Visores de informes externos

Puede utilizar el visor de informes externos para ejecutar un programa externo que genere un informe. El programa externo utiliza la API de TADDM mediante una línea de mandatos para acceder a los datos. Luego el informe se muestra en la interfaz del usuario.

Creación de la lógica del visor de informes externos

Un informe externo se puede implementar dentro de cualquier programa ejecutable. Ejemplos de ello son un script Perl, un script de shell o un programa Java. El programa externo debe generar un archivos HTML válido a través de la salida estándar para que el informe resultante aparezca en el Portal de gestión de datos.

Acerca de esta tarea

Una implementación típica de un visor de informes externos utiliza un script de shell para consultar la API de TADDM y generar los resultados XML de la consulta

en un archivo temporal. Luego el script de shell inicia un procesador XSLT para transformar el resultado de la consulta en salida HTML, que genera salida a STDOUT.

Importante: Los visores de informes externos que utilizan la API de TADDM deben proporcionar credenciales al script `api.sh` de la línea de mandatos en Linux y en UNIX y al archivo `api.bat` en Windows. Puesto que las credenciales son argumentos de la línea de mandatos para el script `api.sh` y `api.bat`, puede que sean visibles para otros usuarios del sistema mediante listas de procesos. Para impedir la revelación de contraseñas sensibles, puede ser útil configurar una cuenta ficticia que tenga acceso de lectura a los objetos que deban aparecer en los informes generados externamente.

El ejemplo siguiente es una implementación simple de un script de shell Bourne de informe externo. Copie el contenido siguiente en un archivo nuevo, `$COLLATION_HOME/sdk/bin/appServers.sh`, y haga que dicho archivo sea legible y ejecutable para el usuario bajo el que se ejecuta el servidor TADDM:

```
#!/bin/sh
# Definir variables de entorno para scripts llamados
export COLLATION_HOME=/opt/ibm/taddm/dist

# Invocar la consulta mediante la API y generar salida en
# $COLLATION_HOME/sdk/bin/appServers.xml
# NOTA: Cambie 'usuario_restringido' y 'contraseña_restringida'
# por las credenciales de su cuenta
ficticias.
sh $COLLATION_HOME/sdk/bin/api.sh -l log -H localhost -u restrictedUser -p
restrictedPassword \ find AppServer > $COLLATION_HOME/sdk/bin/appServers.xml

# Invocar al procesador XSLT
sh $COLLATION_HOME/sdk/bin/xslt.sh -XSL $COLLATION_HOME/sdk/bin/appServers.xsl
```

El siguiente ejemplo pertenece a la hoja de estilo `appServers.xsl` utilizada para transformar el archivo `appServers.xml` generado por el script de shell. El informe muestra los nombres del servidor de aplicaciones y sus versiones de producto. Copie el contenido en un archivo nuevo, `$COLLATION_HOME/sdk/bin/appServers.xsl`, y haga que dicho archivo sea legible para el usuario bajo el que se ejecuta el servidor TADDM.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version = '1.0' xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:coll="urn:www-collation-com:1.0" xmlns:xhtml="http://www.w3.org/1999/xhtml">
        <xsl:variable name="nl">
        <xsl:text>
        </xsl:text>
        </xsl:variable>

        <xsl:variable name="pageheadertext">
                Informe de servidor de aplicaciones simple
        </xsl:variable>

        <xsl:variable name="pagefootertext">
                Fin del informe de servidor de aplicaciones simple
        </xsl:variable>


        <xsl:template match="/">
        <html>
                <head>
                <link rel="stylesheet" type="text/css" media="all"
       href="styles.css" />
                </head>
        <body>
```

```
                <h3>
                        <xsl:value-of select="$pageheadertext"/>
                </h3>
    <table border="1" width="100%">
                 <tr>
                     <th>Versión del producto/th>
                     <th>Nombre/th>
                        </tr>

      <xsl:apply-templates select="document('appServers.xml')/coll:results"/>
    </table>
                <xsl:value-of select="$nl"/>
        </body></html>
        </xsl:template>

        <xsl:template match="coll:AppServer">
                        <tr>
                          <td>xsl:value-of select="coll:productVersion"/></td>
                          <td>xsl:value-of select="coll:displayName"/></td>
                        </tr>
        </xsl:template>
</xsl:stylesheet>
```

Para probar la lógica del informe, ejecute el script `appServer.sh` desde una línea de mandatos. La salida HTML válida se visualiza.

Cómo añadir el visor de informes externos al Portal de gestión de datos

Los informes se añaden al Portal de gestión de datos mediante la modificación del archivo `reports.xml`. El archivo `reports.xml` está situado en el directorio `$COLLATION_HOME/etc/cdm/xml/`.

Procedimiento

Para añadir el visor de informes externos al Portal de gestión de datos, complete los siguientes pasos:

1. Mediante un editor de texto, abra el archivo `$COLLATION_HOME/etc/cdm/xml/reports.xml`.
2. En el archivo `reports.xml`, especifique el descriptor de informes, el grupo de informes, el nombre de los informes y el script externo de la definición de informes. El ejemplo siguiente muestra cómo crear un informe externo llamado `Servidores de aplicaciones` que se encuentra en el grupo `Informes de inventario` y especifica el archivo `sdk/bin/appServers.sh`:

   ```
   <bean class="com.collation.cdm.reports.viewer.ExternalReportViewer" id="AppServers1">
    <property name="reportGroup"><value>Informes de inventario</value></property>
    <property name="reportName"><value>Servidores de aplicaciones</value></property>
    <property name="script"><value>sdk/bin/appServers.sh</value></property>
   </bean>
   ```

3. Guarde el archivo `$COLLATION_HOME/etc/cdm/xml/reports.xml`.
4. Ahora el informe se visualiza en el Portal de gestión de datos.

Visores de informes JSP

Un visor de informes JSP proporciona flexibilidad y seguridad adicionales a los usuarios que dispongan de conocimientos acerca de la creación de Java Server Pages (JSP). La lógica de informes, incluido el acceso de cualquier API, se sitúa en una página JSP que el Portal de gestión de datos representa posteriormente. Al utilizar los visores de informes JSP, las credenciales de seguridad se heredan automáticamente del usuario que ha iniciado sesión.

Creación de la lógica de visor de informes JSP

La lógica de un visor de informes JSP está contenida en un JSP que es llamado por el Portal de gestión de datos. Una implementación típica de un informe JSP utiliza una clase de ayudante de Java denominada TMSDataHelper para consultar la API de TADDM. Los resultados de la consulta son objetos que pueden manipularse utilizando métodos Java. Para obtener más información sobre el modelo y la API de TADDM, consulte la documentación del SDK en `$COLLATION_HOME/sdk/doc`.

Acerca de esta tarea

El ejemplo siguiente es una implementación sencilla del visor de informes JSP. Copie el siguiente contenido en un archivo nuevo, `$COLLATION_HOME/deploy-tomcat/reports.war/WEB-INF/view/custom.jsp` si utiliza TADDM 7.3.0 o `$COLLATION_HOME/apps/reports.war/WEB-INF/view/custom.jsp` si utiliza TADDM 7.3.0.1 y posterior y haga que el archivo sea legible y ejecutable para el usuario que ejecute el servidor TADDM.

El siguiente ejemplo pertenece a la hoja de estilo `appServers.xsl` utilizada para transformar el archivo `appServers.xml` generado por el script de shell. El informe muestra los nombres del servidor de aplicaciones y sus versiones de producto. Copie el contenido en un archivo nuevo, `$COLLATION_HOME/sdk/bin/appServers.xsl`, y haga que dicho archivo sea legible para el usuario que ejecute el servidor de TADDM.

```
<%@ page language="java" %>
<%@ page import="com.collation.cdm.common.util.TMSDataHelper" %>
<%@ page import="java.lang.StringBuffer" %>
<%@ page import="com.collation.cdm.reports.util.ReportsParser" %>
<%@ page import="com.collation.cdm.common.util.TMSReportingTransformer" %>
<%@ page import="com.collation.platform.model.AttributeNotSetException" %>
<%@ page import="com.collation.platform.model.ModelObject" %>
<%@ page import="com.collation.platform.model.topology.sys.ComputerSystem" %>
<%@ page import="com.collation.platform.model.topology.process.BusinessProcess" %>
<%@ page import="com.collation.platform.model.topology.process.Activity" %>
<%@ taglib prefix="x" uri="http://java.sun.com/jstl/xml" %>
<%@ taglib prefix="c" uri="http://java.sun.com/jsp/jstl/core" %>
<%@ page import="com.collation.platform.util.Props" %>
<%@ page import="java.util.ArrayList"%>
<%@ page import="com.collation.cdm.common.messages.CdmLocalizedMessages"%>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%
java.util.Locale locale =
com.collation.cdm.common.util.CDMUtil.checkLocale(request.getLocale());
    if (null == session.getAttribute(org.apache.struts.Globals.LOCALE_KEY)) {
session.setAttribute(org.apache.struts.Globals.LOCALE_KEY, locale);
    }
%>
<%
// TMSDataHelper es una clase de utilidad para ejecutar
// consultas MQL en la base de datos
TMSDataHelper tms = new TMSDataHelper(locale);

//Ejecute una consulta para todos los sistemas informáticos
ModelObject dataIn[] = tms.doModelObjectQuery("SELECT * FROM ComputerSystem",null);

  //Genere un informe HTML basado en la salida de la API
  StringBuffer output = new StringBuffer();
  output.append("<p>");
  output.append("<table border=\"1\">");
                int c = 0;
                int s = dataIn.length;
                while (cs) {
```

```
                        ComputerSystem tmo = (ComputerSystem)dataIn[c];
                        String csName = null;
                        String csLabel = null;
                        if (tmo.hasName()) {
                                try {
                                        csName = tmo.getName();
                                } catch (AttributeNotSetException e) {
                                        csName = "unknown";
                                }
                        }
                        if (tmo.hasSignature()) {
                                try {
                                        csLabel = tmo.getSignature();
                                } catch (AttributeNotSetException e) {
                                        csLabel = "";
                                }
                        }
                        output.append("<tr><td colspan=\"2\" bgcolor=\"#9999FF\">");
                        output.append("ComputerSystem" + "<br>");
                        output.append(" Name: " + csName + "<br>");
                        output.append("</td><td>");
                        output.append("Signature: " + csLabel);
                        output.append("</td></tr>");
                        c++;
                }
output.append("</table>");
String bpstring = output.toString();
%>
<html>
<body>
<h1>Sample JSP Report/h1>
<%=bpstring%>
</body>
</html>
```

Cómo añadir el visor de informes JSP al Portal de gestión de datos

Los informes se añaden al Portal de gestión de datos mediante la modificación del archivo `reports.xml`. El archivo `reports.xml` está ubicado en el directorio `$COLLATION_HOME/etc/cdm/xml/`.

Procedimiento

Para añadir el visor de informes JSP al Portal de gestión de datos, complete los siguientes pasos:

1. Mediante un editor de texto, abra el archivo `$COLLATION_HOME/etc/cdm/xml/reports.xml`.
2. En el archivo `reports.xml`, especifique el descriptor de informes, el grupo de informes, el nombre de los informes y el script externo de la definición de informes. El ejemplo siguiente muestra cómo crear un informe externo llamado `Informe personalizado` que se encuentre en el grupo `Informes de inventario` y especifique el script `/WEB-INF/view/custom.jsp`:

   ```
   <bean class="com.collation.cdm.reports.viewer.JSPReportViewer" id="CustomReport">
    <property name="reportGroup"><value>Informes de inventario</value></property>
    <property name="reportName"><value>Informe personalizado</value></property>
    <property name="script"><value>/WEB-INF/view/custom.jsp</value></property>
   </bean>
   ```

3. Guarde el archivo `$COLLATION_HOME/etc/cdm/xml/reports.xml`.
4. Ahora el informe debería aparecer en el Portal de gestión de datos.

Creación de informes con Tivoli Common Reporting

Como visualizar los informes de BIRT en BIRT Report Viewer no es seguro y está inhabilitado de forma predeterminada, puede importar los informes de BIRT para TADDM a Tivoli Common Reporting. Esto habilita los informes de varios productos que incluyen datos de TADDM. También puede utilizar las características de Tivoli Common Reporting como la planificación de informes, o utilizar Tivoli Common Reporting como repositorio central para los informes.

Para algunas tareas, los pasos que deba completar diferirán en función de la versión de Tivoli Common Reporting o de la base de datos que esté utilizando.

Fix Pack 1 Si tiene TADDM 7.3 Fix Pack 1 o posterior, consulte también la guía de mejores prácticas El modelo Cognos mejorado en TADDM 7.3 FP*x*.

Visión general de Tivoli Common Reporting

La herramienta Tivoli Common Reporting es una función de creación de informes que se proporciona con determinados productos de Tivoli y que ofrece un método centralizado para visualizar y administrar informes con un aspecto consistente en distintos productos.

Tivoli Common Reporting incluye un almacén de datos para almacenar y organizar informes e interfaces para gestionar, ejecutar, planificar y visualizar informes. Tivoli Common Reporting utiliza los motores de tiempo de ejecución Cognos y BIRT.

Importante: Tivoli Common Reporting se proporciona en el disco de instalación de IBM Jazz for Service Management. Si no tiene pensado instalar IBM Jazz for Service Management, puede utilizar la capacidad de informes BIRT integrada.

Si ya tiene Tivoli Common Reporting instalado en el sistema, opcionalmente puede, importar los informes de TADDM predefinidos, que son compatibles con Tivoli Common Reporting. Luego puede utilizar Tivoli Common Reporting como repositorio central para los informes del producto Tivoli. También puede utilizar las opciones avanzadas de creación de informes, incluidas la creación de informes para varios productos, la seguridad basada en roles y la planificación de informes.

Para ver las versiones soportadas de los productos, vaya a la sección “Versiones soportadas” en la página 200.

Nota: Si utiliza TADDM con IBM Tivoli Change and Configuration Management Database (CCMDB) o IBM SmartCloud Control Desk, consulte las documentaciones de CCMDB o IBM SmartCloud Control Desk para obtener información sobre qué versiones de Tivoli Common Reporting están soportadas.

Para obtener más información sobre Tivoli Common Reporting, diríjase a https://www.ibm.com/developerworks/community/groups/service/html/communityview?communityUuid=9caf63c9-15a1-4a03-96b3-8fc700f3a364.

Instalación de Tivoli Common Reporting e IBM Cognos Framework Manager

Debe instalar Tivoli Common Reporting e IBM Cognos Framework Manager.

Procedimiento

Para instalar Tivoli Common Reporting e IBM Cognos Framework Manager, siga estos pasos:

1. Instale Tivoli Common Reporting con las opciones predeterminadas que se le presenten. Si utiliza una base de datos Oracle, debe utilizar Tivoli Common Reporting 2.1 o 3.1.
2. Instale el paquete de IBM Cognos Framework Manager que está disponible en la carpeta `CognosModeling`. Utilice las opciones predeterminadas que se le presenten.
3. Si está disponible, instale también el parche de seguridad disponible en la carpeta `CognosModelingFix`. Utilice las opciones predeterminadas que se le presenten.

Instalación y configuración del cliente de base de datos

Si ha instalado Tivoli Common Reporting en un sistema distinto del servidor de bases de datos de TADDM, deberá instalar un cliente de base de datos para conectar con la base de datos. Puede utilizar un cliente de base de datos DB2 u Oracle, en función del tipo de base de datos TADDM. Si ha instalado Tivoli Common Reporting en el mismo servidor que la base de datos TADDM, no es necesario que instale un cliente de base de datos.

Procedimiento

Para instalar y configurar el cliente de base de datos, siga estos pasos:

Realice una de las tareas siguientes:

- Si desea utilizar el cliente de base de datos DB2, complete los siguientes pasos:
  1. Instale el cliente de DB2 en la máquina en la que está instalado TCR utilizando las opciones predeterminadas que se le presenten.
  2. Asegúrese de que la base de datos de TADDM se haya catalogado. Este paso es necesario para que Tivoli Common Reporting se conecte correctamente al servidor de DB2 mediante el cliente de DB2.
- Si desea utilizar el cliente de base de datos Oracle, realice los pasos siguientes para instalarlo y configurarlo utilizando el asistente Oracle Universal Installer y el asistente Oracle Net Configuration Assistant:
  1. En la página Select Installation Type (Seleccionar tipo de instalación) del asistente Oracle Universal Installer, seleccione **Administrator** como la modalidad de instalación.
  2. En la página Specify Home Details (Especificar detalles de inicio), especifique el nombre de la instalación y la vía de acceso a la ubicación en la que desea instalar el producto.
  3. En la página Product-Specific Prerequisite Checks (Comprobaciones de requisitos previos específicos del producto), asegúrese de que se cumplan todos los requisitos para la instalación y la configuración. No continúe con la instalación hasta que cada comprobación tenga un estado **Correcto**.
  4. En la página Bienvenida del asistente Oracle Net Configuration Assistant, asegúrese de que el recuadro de selección **Perform typical configuration** (Realizar configuración típica), no esté marcado.
  5. En la página Naming Methods Configuration, Select Naming Method (Configuración de métodos de nombres, Seleccionar método de nombre), establezca **Local Naming** (Nombres locales) como el método para asignar nombres.
  6. En la página Net Service Name Configuration, Service Name (Configuración de nombres del servicio de red, Nombre de servicio), escriba el nombre de servicio para el servidor de base de datos de Oracle, por ejemplo, `ORCL`.

7. En la página Net Service Name Configuration, Select Protocols (Configuración de nombres del servicio de red, Seleccionar protocolo), seleccione **TCP** como el protocolo que se ha de utilizar para conectar con la base de datos.
8. En la página Net Service Name Configuration, TCP/IP Protocol (Configuración de nombres del servicio de red, Protocolo TCP/IP), escriba el nombre de host del sistema en el que se ejecuta la base de datos. Seleccione **Use the standard port number of 1521** (Utilizar el número de puerto estándar 1521).
9. En la página Net Service Name Configuration, Test (Configuración de nombres del servicio de red, Prueba), seleccione **Yes, perform a test** (Sí, realizar una prueba).

   Si el nombre de usuario y la contraseña de la base de datos son correctos, se muestra el texto siguiente:

   ```
   Connecting... Test successful.
   ```

   Si no se realiza una conexión correcta con la base de datos, es posible que tenga que cambiar las credenciales de inicio de sesión. Para cambiar las credenciales de inicio de sesión, pulse en **Change Login** (Cambiar inicio de sesión) y especifique un nombre de usuario y una contraseña de base de datos válidos.
10. En la página Net Service Name Configuration, Net Service Name (Configuración de nombres del servicio de red, Nombre de servicio de red), acepte el nombre de servicio predeterminado, que debería ser el nombre de servicio especificado anteriormente.
11. Cree una variable de sistema de Windows llamada `TNS_ADMIN` y defina el valor como la vía de acceso completa de la carpeta que contiene el archivo `tnsnames.ora`. Durante la instalación, el archivo `tnsnames.ora` se crea en la carpeta `%ORACLE_HOME%/client_1/NETWORK/ADMIN`, por ejemplo `C:/oracle/product/10.2.0/client_1/NETWORK/ADMIN`.
12. Defina la variable `TNS_ADMIN` que se encuentra en el script `startTCRserver.sh/bat` para que apunte a la ubicación del archivo `tnsnames.ora`, por ejemplo `%ORACLE_HOME%/client_1/NETWORK/ADMIN`.
13. Reinicie el sistema para asegurarse de que la nueva variable del sistema está disponible.

Configuración de IBM Cognos Framework Manager

Debe actualizar las propiedades de IBM Cognos 10 Framework Manager con los valores adecuados.

Acerca de esta tarea

Nota: El siguiente procedimiento se aplica a la configuración de IBM Cognos 10 Framework Manager para Tivoli Common Reporting 3.1. Sin embargo, es el mismo para IBM Cognos 8 Framework Manager para Tivoli Common Reporting 2.1.

Cuando se instala Tivoli Common Reporting, se instala el programa IBM Cognos Configuration y se actualizan los valores de algunas propiedades. Cuando se instala IBM Cognos 10 Framework Manager, se instala una versión diferente del programa IBM Cognos Configuration, pero no se actualizan todas las propiedades. Es necesario copiar manualmente los valores de algunas propiedades de la versión de Tivoli Common Reporting del programa IBM Cognos Configuration a la versión de IBM Cognos 10 Framework Manager del programa IBM Cognos Configuration.

Procedimiento

Para configurar IBM Cognos 10 Framework Manager, complete los siguientes pasos:

1. Abra la versión de IBM Cognos Configuration instalada por Tivoli Common Reporting. Para abrir este programa, pulse en **Inicio** > **Programas** > **Tivoli Common Reporting 3.1** > **IBM Cognos Configuration**.
2. Abra la versión de IBM Cognos Configuration instalada por IBM Cognos 10. Para abrir este programa, pulse en **Inicio** > **Programas** > **IBM Cognos 10** > **IBM Cognos Configuration**.
3. Para cada versión de IBM Cognos Configuration, pulse en **Configuración local** > **Entorno**.
4. Copie el valor de la propiedad del **URI de pasarela** de la versión de Tivoli Common Reporting de IBM Cognos Configuration a la propiedad **URI de pasarela** de la versión de IBM Cognos 10 de IBM Cognos Configuration. La sintaxis del URI es: `http://tcrhost:16310/tarf/servlet/dispatch`.
5. Copie el valor de la propiedad **URI de asignador externo** de la versión de Tivoli Common Reporting de IBM Cognos Configuration a la propiedad **URI de asignador para aplicaciones externas** de la versión de IBM Cognos 10 de IBM Cognos Configuration. La sintaxis del URI es: `http://tcrhost:16310/tarf/servlet/dispatch`.
6. Guarde los cambios realizados en la versión IBM Cognos 10 de IBM Cognos Configuration.

Generación del modelo de TADDM

Fix Pack 1

Puede generar el modelo de TADDM para tener la instantánea actualizada del contenido de la base de datos de TADDM, incluidas las definiciones de todos los atributos ampliados. Si no utiliza atributos ampliados puede saltar este procedimiento y utilizar el archivo de modelo predefinido de TADDM Cognos, el archivo `$COLLATION_HOME/etc/reporting/tcr/model.xml`.

Antes de empezar

El modelo de TADDM generado incluye todas las clases de modelo de datos comunes que admite TADDM y las definiciones de atributos ampliados almacenadas en la base de datos de TADDM. Puede publicar el modelo de TADDM en el servidor de Tivoli Common Reporting y utilizarlo en los informes de Cognos. Puede generar el modelo de TADDM muchas veces. Cada vez que vuelva a generar el modelo, este incluirá el contenido actualizado de la base de datos de TADDM.

Notas:

- Si se eliminan las definiciones de atributos ampliados de la base de datos de TADDM tras publicar el modelo de TADDM en el servidor de Tivoli Common Reporting, los informes de Cognos que las utilicen pueden dejar de funcionar.
- Si utiliza el sistema operativo Windows, cambie la extensión de los scripts utilizados en el siguiente procedimiento de `.sh` a `.bat`.

Procedimiento

1. En el servidor de TADDM, abra el directorio `$COLLATION_HOME/bin`.
2. Renueve las vistas de atributos ampliados llevando a cabo los siguientes pasos:

a. Si ha creado alguna vista de atributos ampliados, elimínela ejecutando el siguiente mandato:
   ```
   ./extattr_views.sh remove
   ```
b. Genere scripts SQL con definiciones de vistas de atributos ampliados ejecutando el siguiente mandato:
   ```
   ./extattr_views.sh scripts
   ```
c. Cree las vistas de atributos ampliados mediante los scripts SQL generados ejecutando el siguiente mandato:
   ```
   ./extattr_views.sh create
   ```

3. Para generar el archivo de modelo de Cognos, ejecute el siguiente mandato:
   ```
   ./genCognosModel.sh
   ```
   El modelo de TADDM generado se almacena en el archivo `model.xml` y se coloca en el directorio ⌂`$COLLATION_HOME/etc/reporting/tcr`. Los mensajes de registro del mandato están en el archivo `$COLLATION_HOME/log/genCognosModel.log`.

Qué hacer a continuación

Puede publicar el modelo de TADDM generado en el servidor de Tivoli Common Reporting mediante IBM Cognos Framework Manager. Para obtener más información, consulte "Publicación del modelo utilizando IBM Cognos Framework Manager" en la página 172.

Para obtener más información sobre las vistas de atributos ampliados, consulte el tema *Vistas de atributos ampliados* de la *Guía del desarrollador SDK* de TADDM.

Importación de los informes de modelos y de ejemplo a Tivoli Common Reporting

Puede importar informes de TADDM de ejemplo a Tivoli Common Reporting versión 2.1 y 3.1.

Acerca de esta tarea

Este procedimiento se aplica a **Tivoli Common Reporting versión 2.1**.

Procedimiento

Para importar informes de modelos y de ejemplo a Tivoli Common Reporting 2.1, complete los siguientes pasos:

1. Copie el paquete `$COLLATION_HOME/etc/reporting/TADDMPackage.zip` del servidor de TADDM a la carpeta `TCRComponent/cognos/deployment` del servidor de Tivoli Common Reporting.
2. Abra la página de inicio de Tivoli Common Reporting.
3. Pulse **Informes** > **Common Reporting**.
4. En el menú **Iniciar**, seleccione **Administración**. Se muestra el panel Administración.
5. Pulse el separador **Configuración**.
6. Pulse en el icono **Nueva importación**. El asistente de Nueva importación se visualiza.
7. En la lista de paquetes disponibles, seleccione **TADDMPackage**. Pulse **Siguiente**.

8. Opcional: En el campo **Descripción**, escriba una descripción del paquete. Pulse **Siguiente**.
9. Seleccione el recuadro de selección situado junto al nombre del paquete.
10. En la sección **Opciones**, pulse en **El propietario del origen** y **Entradas nuevas y existentes**. En el menú **Nivel de registro**, seleccione **Básico**. Pulse **Siguiente**.
11. Pulse **Guardar y ejecutar una vez**. Pulse **Siguiente**.

Acerca de esta tarea

Este procedimiento se aplica a **Tivoli Common Reporting versión 3.1**.

Procedimiento

Para importar informes de modelos y de ejemplo a Tivoli Common Reporting 3.1, complete los siguientes pasos:

1. Copie el paquete `$COLLATION_HOME/etc/reporting/TADDMPackage.zip` del servidor de TADDM a la carpeta `reporting/cognos/deployment` de JazzSM installation.
2. Abra la página de inicio de Tivoli Common Reporting.
3. Pulse **Informes** > **Common Reporting**.
4. En el menú **Iniciar**, seleccione **IBM Cognos Administration**. Se muestra el panel Administración.
5. Pulse el separador **Configuración**.
6. Vaya a Administración de contenido. Pulse el icono **Nueva importación**. El asistente de Nueva importación se visualiza.
7. En la lista de paquetes disponibles, seleccione **TADDMPackage**. Pulse **Siguiente**.
8. Opcional: En el campo **Descripción**, escriba una descripción del paquete. Pulse **Siguiente**.
9. Seleccione el recuadro de selección situado junto al nombre del paquete. Pulse **Siguiente**.
10. En la sección **Propiedad de entrada**, pulse en **El propietario del origen** y **Entradas nuevas y existentes**. En el menú **Nivel de registro** de la sección **Registro de despliegue**, seleccione **Básico**. Pulse **Siguiente**.
11. Compruebe que los valores que se han proporcionado sean correctos. Pulse **Siguiente**.
12. Pulse **Guardar y ejecutar una vez**. Pulse **Finalizar**.
13. Pulse **Ejecutar**.

Vistas de datos en el modelo de TADDM

Puede generar informes desde el archivo de modelo de datos de TADDM, `model.xml`.

El modelo de datos está organizado en varios espacios de nombres. El espacio de nombres es un contenedor lógico en el que todos los nombres son exclusivos. Cada espacio de nombres contiene asuntos de consulta, elementos de consulta y objetos. Los siguientes espacios de nombres siguen presentes tras importar el archivo `model.xml` de TADDM:

Fix Pack 1 **Espacio de nombres CDM**

Estas vistas contienen los asuntos de consulta de casi todas las clases del modelo de datos comunes, incluidas las clases relacionadas con el

descubrimiento, divididas en varios espacios de nombres por sus nombres de paquete. Los nombres de paquete se ordenan alfabéticamente. Las clases de modelo simplificado se distinguen por el prefijo `simple` en el nombre del espacio de nombres. Puede utilizar estos datos para generar informes que contengan distintos tipos de objetos CDM.

Los asuntos de consulta de los nombres de espacio de CDM contienen relaciones predefinidas que se relacionan con los atributos `Parent`. Por ejemplo, la clase `app.j2ee.J2EEDomain` tiene el atributo `Servers` del tipo `app.j2ee.J2EEServer[]`. Asimismo, la clase `app.j2ee.J2EEServer` tiene el atributo `Parent` del tipo `app.j2ee.J2EEDomain`. Por lo tanto, entre todos los pares compatibles de clases de CDM hay relaciones predefinidas, como por ejemplo:

- `app.j2ee.J2EEDomain [0..1] - [0..n] app.j2ee.J2EEServer`
- `app.j2ee.J2EEDomain [0..1] - [0..n] app.j2ee.jboss.JBossServer`
- `app.j2ee.J2EEDomain [0..1] - [0..n] app.j2ee.weblogic.WebLogicServer`
- `app.j2ee.jboss.JBossDomain [0..1] - [0..n] app.j2ee.jboss.JBossServer`
- `app.j2ee.websphere.WebSphereCell [0..1] - [0..n] app.j2ee.websphere.WebSphereServer`

En TADDM 7.3.0.1, algunos asuntos de consulta de los nombres de espacios de CDM se definen para atributos no persistentes del tipo de matriz. En TADDM 7.3.0.2, los asuntos de consulta se definen para todos los atributos del tipo de matriz. Sus nombres tienen el siguiente formato: "*[nombre de la clase que declara el atributo matriz]-->[nombre del atributo matriz]*". Por ejemplo, la clase `simple.SGroup` tiene el atributo `GroupMembers` del tipo `ModelObject[]`, por lo que el asunto de consulta es `"SGroup-->GroupMembers"`. Estos asuntos de consulta contienen relaciones predefinidas entre los atributos matriz descritos y todas las clases de CDM que contienen dichos atributos. Por ejemplo, para el atributo mencionado `GroupMembers` se definen, entre otras, las siguientes relaciones:

- `simple.SGroup [1..1] - [0..n] simple."SGroup-->GroupMembers"`
- `simple.SBaseCollection [1..1] - [0..n] simple."SGroup-->GroupMembers"`
- `app.biztalk.BizTalkGroup [1..1] - [0..n] simple."SGroup-->GroupMembers"`
- `app.hacmp.HACMPResourceGroup [1..1] - [0..n] simple."SGroup-->GroupMembers"`

Para utilizar los atributos del tipo de matriz, debe definir una relación entre un atributo del tipo de matriz y la clase CDM necesaria utilizando su atributo `PK_C` o, en caso del atributo no persistente del tipo de matriz (`ModelObject[]`), su atributo `Guid`. Por ejemplo:

- Fix Pack 2 Para crear un informe Cognos que muestra los objetos `sys.zOS.ZReportFile` como `ZReportfiles` de los objetos `sys.ComputerSystem`, debe definir una unión entre las columnas siguientes en IBM Cognos Report Studio:

  ```
  sys."ComputerSystem-->ZReportfiles".PK__ZReportfiles_C
   [0..n]-[0..1] sys.zOS.ZReportFile.PK_C
  ```

- Para crear un informe Cognos que muestra los objetos `app.AppServer` como `GroupMembers` de los objetos `simple.SBaseCollection`, debe definir una unión entre las siguientes columnas en IBM Cognos Report Studio:

```
simple."SGroup-->GroupMembers".GroupMembersGuids [0..n]-
[0..1] app.AppServer.Guid
```

Fix Pack 2 En muchos casos, no es necesario crear manualmente uniones para los atributos del tipo de matriz, ya que existen atributos `Padre` de los objetos dependientes correspondientes. El modelo Cognos contiene relaciones para los mismos. Por ejemplo, no es necesario que cree manualmente uniones para crear un informe que muestra objetos `sys.FileSystem` como `FileSystems` de los objetos `sys.ComputerSystem`, debido a que los objetos `sys.FileSystem` tienen el atributo `Padre` que apunta a los objetos `sys.ComputerSystem`.

Fix Pack 3 En TADDM 7.3.0.3 y posterior, el modelo de Cognos contiene elementos de consulta de tipo `Data Time` para todos los atributos de tipo de indicación de fecha y hora. Por ejemplo, el asunto de consulta `sys.aix.AixUnitaryComputerSystem` contiene los siguientes elementos de consulta:

- `LastStoredTime` del tipo `Int64`, que apunta a la columna LASTSTOREDTIME_C en la vista de bloques de creación. Valor de ejemplo de la columna: `1445417251307`.
- `LastStoredTimeT` del tipo `Data Time`, que apunta a la columna LASTSTOREDTIME_T en la vista de bloques de creación. Valor de ejemplo en la columna: `Oct 21, 2015 10:47:31 AM`.

El elemento de consulta `LastStoredTimeT` es el equivalente del elemento de consulta `LastStoredTime`, solo que se expresa en el formato Tiempo universal coordinado, en lugar del tiempo UNIX (entero largo). Los elementos de consulta que contienen el sufijo `T` son los equivalentes de la indicación de fecha y hora del atributo entero largo original.

Espacio de nombres de WebSphere

Nota: Fix Pack 1 Espacio de nombre de WebSphere está en desuso en TADDM 7.3.0.1 y posterior.
Esta vista contiene los asuntos de consulta primarios para un entorno WebSphere. Puede utilizar estos datos para generar informes específicos de WebSphere, como listados de propiedades o valores de JVM de servidores WebSphere. Este tema de consulta de `Servidor WebSphere` está enlazado con el asunto de consulta de `AppServer` incluido en el espacio de nombres compartido. Los asuntos de consulta del `clúster de WebSphere` y de la `celda de WebSphere` están enlazados con los asuntos de consulta del `clúster de AppServer` y del `Dominio de J2EE` incluidos en el espacio de nombres compartido.

Espacio de nombres compartido

Nota: Fix Pack 1 Espacio de nombre compartido está en desuso en TADDM 7.3.0.1 y posterior.
Esta vista contiene asuntos de consulta que se consideran clases de clave y se pueden utilizar como puente para unir datos entre distintos espacios de nombres. El espacio de nombres compartido contiene información sobre sistemas informáticos y clases de colección. Puede utilizar estos datos para crear informes de inventario.

Espacio de nombres de aplicaciones empresariales

Nota: Fix Pack 1 Espacio de nombre de aplicaciones empresariales está en desuso en TADDM 7.3.0.1 y posterior.
Esta vista contiene asuntos de consulta para una aplicación empresarial, es decir, los asuntos de consulta `Aplicación` y `Grupo funcional`. El asunto de consulta de grupo funcional está enlazado con el espacio de nombres compartido a través del tema de consulta `Colección`. Puede utilizar estos datos para crear informes que muestren aplicaciones empresariales y sus miembros.

Espacio de nombres de base de datos

Nota: Fix Pack 1 Espacio de nombre de base de datos está en desuso en TADDM 7.3.0.1 y posterior.
Esta vista contiene asuntos de consulta relacionados con bases de datos y servidores de bases de datos. Puede utilizar el asunto de consulta `Todas las bases de datos` para generar informes de bases de datos generales en lugar de informes de bases de datos específicos de un proveedor. El contenido de la base de datos está enlazado con el espacio de nombres compartido a través del asunto de consulta `AppServers`.

Espacio de nombres de dependencias y relaciones

Nota: Fix Pack 1 Espacio de nombre de dependencias y relaciones está en desuso en TADDM 7.3.0.1 y posterior.
Esta vista contiene asuntos de consulta que representan relaciones y dependencias generadas, tales como dependencias de IP o relaciones de conmutador a dispositivo. Puede utilizar el asunto de consulta `relación (sin enlazar)` de propósito general para crear enlaces manuales al crear un informe o consulta. El tema de consulta `Conmutador a dispositivo` une conmutadores con objetos de sistema informático en el espacio de nombres compartido. Hay tres asuntos de consulta relacionados con la afinidad de servidor. El tema de consulta `Servidor` muestra la unión de todos sistemas informáticos, servidores de aplicaciones y objetos de servicio de la base de datos. El asunto de consulta `Afinidad (vinculada a destino)` une cada relación de afinidad con su destino en el asunto de consulta `Servidor`. El asunto de consulta `Afinidad (vinculada a origen)` une cada relación de afinidad con su origen en el asunto de consulta `Servidor`. El contenido del servidor está enlazado con el espacio de nombres compartido a través del sistema informático, el servidor de aplicaciones y los asuntos de consulta de servicio. Puede utilizar estos datos para generar un informe general que muestre la relación entre elementos de configuración de la red.

Publicación del modelo utilizando IBM Cognos Framework Manager

Si desea añadir objetos al modelo de datos de TADDM (archivo `model.xml`), es necesario editar el archivo y luego importarlo mediante IBM Cognos 10 Framework Manager.

Acerca de esta tarea

El siguiente procedimiento se aplica a IBM Cognos 10 Framework Manager. Sin embargo, es el mismo para IBM Cognos 8 Framework Manager.

Procedimiento

Para importar el modelo de datos mediante IBM Cognos 10 Framework Manager, siga estos pasos:

1. Inicie IBM Cognos 10 Framework Manager.
2. Cree una proyecto nuevo.
3. Cuando se le solicite, escriba las credenciales para el servidor de Tivoli Common Reporting. Es posible que se le soliciten las credenciales más de una vez.
4. Cierre IBM Cognos 10 Framework Manager.
5. Copie el archivo siguiente desde el servidor de TADDM a la carpeta del proyecto de Cognos Framework:

   ```
   $COLLATION_HOME/etc/reporting/tcr/model.xml
   ```

   Sobrescriba el archivo `model.xml` que hay en la carpeta del proyecto de Cognos Framework.
6. Inicie IBM Cognos 10 Framework Manager y abra el proyecto que ha creado antes.
7. En el panel Visor de proyectos, pulse en **Orígenes de datos** > ***nombre_origen_datos_gestor_contenido***.
8. Si utiliza una base de datos de DB2 con un nombre diferente en lugar del que está definido en el origen de base de datos de Cognos, sustituya el contenido del campo **Esquema** por el nombre de la instancia de DB2 utilizado para la base de datos de TADDM.
9. Guarde el proyecto.
10. En el panel Visor de proyectos, pulse en **Paquetes**.
11. Pulse con el botón derecho en el nombre del paquete y seleccione **Publicar paquetes**. La verificación y la publicación del modelo TADDM Cognos pueden tardar varios minutos.

Configuración del origen de datos en Tivoli Common Reporting

Puede utilizar Tivoli Common Reporting para configurar el origen de datos.

Antes de empezar

Asegúrese de que se cumple alguna de las condiciones siguientes:

- La base de datos de TADDM está catalogada localmente.
- Tivoli Common Reporting se está ejecutando en el servidor que aloja la base de datos de TADDM.

Si utiliza una base de datos DB2, compruebe que el nombre de esquema coincida con el nombre de instancia de DB2. El nombre del esquema especifica el nombre de la base de datos de DB2 que se utiliza para autorizar el acceso a la base de datos especificada. El nombre de instancia de DB2 se especifica durante la instalación de TADDM. El nombre de instancia predeterminado especificado en el archivo `model.xml` de TADDM es `DB2INST1`. Si es necesario, cambie el nombre del esquema.

Si se utiliza una base de datos Oracle, asegúrese de que el nombre de esquema esté en blanco.

Procedimiento

Para configurar el origen de datos utilizando Tivoli Common Reporting, complete los pasos siguientes:

1. Abra la página de inicio de Tivoli Common Reporting.
2. Pulse **Informes** > **Common Reporting**.
3. En el menú **Iniciar**, en función de la versión de Tivoli Common Reporting que utiliza, seleccione uno de los siguientes elementos de menú:
   - Versión 2.1 - **Administration**.
   - Versión 3.1 - **IBM Cognos Administration**.

   Se muestra el panel Administración.
4. Pulse el separador **Configuración**.
5. Pulse en el icono **Nuevo origen de datos**. Se visualiza el asistente Nuevo origen de datos.
6. En el campo **Nombre**, escriba `CMDBTCR`. Se hace referencia al nombre `CMDBTCR` en el modelo de datos, por lo que debe asignar el mismo nombre al nuevo origen de datos.
7. En el menú **Tipo**, seleccione el tipo de base de datos que está utilizando.
8. Efectúe uno de los pasos siguientes:
   - Si el tipo de su base de datos es DB2, en el campo **Nombre de base de datos DB2**, escriba el nombre de la base de datos de TADDM o el alias de la base de datos TADDM catalogada.
   - Si el tipo de base de datos es Oracle, en el campo **Serie de conexión SQL*Net**, escriba el nombre de servicio de la base de datos Oracle como, por ejemplo, `ORCL`. El nombre de servicio de la base de datos Oracle se ha especificado al configurar el cliente de base de datos Oracle. Puede comprobar el nombre de servicio de la base de datos Oracle en el archivo `%TNS_ADMIN%/tnsnames.ora`. Busque la serie siguiente:

     ```
     SERVICE_NAME =
     ```
9. En la sección **Inicio de sesión**, especifique el nombre de usuario y la contraseña de la base de datos.
10. Para probar la conexión de base de datos, pulse en **Probar**. En la página Ver resultados del asistente de Nuevo origen de datos se muestra el estado de la prueba.

Importación del paquete de informe de TADDM a Tivoli Common Reporting

Para importar los informes predefinidos de TADDM a Tivoli Common Reporting, puede importar el paquete de informe de TADDM.

Antes de empezar

En primer lugar, debe tener la función Tivoli Common Reporting instalada en el sistema. Tivoli Common Reporting se proporciona con algunos productos de Tivoli, pero actualmente no se incluye con TADDM.

Acerca de esta tarea

Un *paquete de informe* de Tivoli Common Reporting es un archivo .zip que contiene uno o varios informes o diseños de informes junto con los recursos que estos necesitan, en un formato que Tivoli Common Reporting puede utilizar. Los

informes de BIRT predefinidos para TADDM se proporcionan en un paquete de informe que puede importar a Tivoli Common Reporting.

Para algunos informes de BIRT hay distintas versiones del mismo informe disponibles en función del servidor en el que se esté ejecutando el informe; por ejemplo, el informe TADDM_SNAPSHOT_CHANGE en el servidor de dominio o servidor de almacenamiento, y el informe TADDM_SNAPSHOT_SYNC_CHANGE en el servidor de sincronización. Generalmente solo está disponible la versión adecuada de un informe, pero después de importar informes de BIRT a Tivoli Common Reporting, puede que ambas versiones del informe estén disponibles. Asegúrese de utilizar únicamente la versión del informe que resulte apropiada para el servidor en el que desea ejecutarlo.

Después de importar informes de BIRT a Tivoli Common Reporting, es posible que haya disponibles varios informes con el texto "Drill-through only" (Solo acceso a detalles) en el nombre del informe. Estos informes están concebidos para ejecutarse para acceder a los detalles de los datos seleccionados en otro informe y no deben ejecutarse por separado.

El informe de afinidad de servidores por ámbito no se puede importar a Tivoli Common Reporting.

Para obtener más información acerca de la importación de paquetes de informes, consulte la documentación de Tivoli Common Reporting.

Procedimiento

Para importar informes de TADDM, complete los siguientes pasos:

1. Si utiliza Tivoli Common Reporting 1.3, complete los siguientes pasos:
   a. En la ventana de navegación de informes de Tivoli Common Reporting, diríjase al separador **Navegación**.
   b. Pulse con el botón derecho del ratón en el nodo raíz del árbol de navegación (Conjuntos de informes).
   c. Pulse en **Importar paquete de informe**.
   d. En la ventana Importar paquete de informe, especifique la ubicación del archivo de paquete de informe `TADDMReports.zip`. Este archivo está ubicado en el directorio `$COLLATION_HOME/etc/reporting`.
   e. Expanda **Opciones avanzadas** y realice lo siguiente:
      1) Seleccione el recuadro de selección **Sobrescribir**. Esto asegura que cualquier copia de los informes instalada anteriormente se sobrescriba.
      2) En el campo **Conjunto de seguridad**, escriba el nombre del conjunto de seguridad al que desea importar el contenido del paquete de informe.
   f. Pulse en **Importar**. El paquete de informe de TADDM se importa al almacén de datos de Tivoli Common Reporting.
2. Si se utiliza Tivoli Common Reporting 2.1, complete los siguientes pasos:
   a. Abra una línea de mandatos y navegue hasta `TIP_install_dir/tipv2Components/TCRComponent/bin`.
   b. Ejecute el mandato de importación:

      ```
      trcmd -user ID_usuario -password contraseña -import -bulk archivo_paquete
      ```

      donde *archivo_paquete* es la vía de acceso al archivo de paquete de informe `TADDMReports.zip` copiado al servidor de Tivoli Common Reporting desde `$COLLATION_HOME/etc/reporting` en el servidor TADDM.

c. El paquete de informe de TADDM se importa al almacén de datos de Tivoli Common Reporting.

3. Si se utiliza Tivoli Common Reporting 3.1, complete los siguientes pasos:
   a. Abra una línea de mandatos y navegue hasta `JazzSM_install_dir/reporting/bin`.
   b. Ejecute el mandato de importación:

      ```
      trcmd -user ID_usuario -password contraseña -import -bulk archivo_paquete
      ```

      donde *archivo_paquete* es la vía de acceso al archivo de paquete de informe `TADDMReports.zip` copiado al servidor de Tivoli Common Reporting desde `$COLLATION_HOME/etc/reporting` en el servidor TADDM.
   c. El paquete de informe de TADDM se importa al almacén de datos de Tivoli Common Reporting.

Qué hacer a continuación

Tras haber importado los informes de TADDM, es necesario volver a configurar el origen de datos JDBC correspondiente a cada informe.

Configuración de informes de BIRT de TADDM en Tivoli Common Reporting

Tras haber importado los informes de TADDM a Tivoli Common Reporting, debe configurar el origen de datos JDBC que utiliza cada informe.

Antes de empezar

Antes de configurar el acceso de JDBC, asegúrese de que se han instalado los archivos de controlador JDBC adecuados en el directorio de controladores de Tivoli Common Reporting. Para Tivoli Common Reporting 1.3 se encuentran en el directorio siguiente:

```
dir_instalación_tcr/products/tcr/lib/birt-runtime-2_2_1/ReportEngine/plugins/
  org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers
```

Para Tivoli Common Reporting 2.1 se encuentran en el directorio siguiente:

```
dir_install_tip/tip21Components/TCRComponent/lib/birt-runtime-2_2_2/ReportEngine/plugins/
org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers
```

Para Tivoli Common Reporting 3.1 se encuentran en el directorio siguiente:

```
JazzSM_install_dir/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/
org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers
```

Si utiliza una base de datos Oracle, asegúrese de que `ojdbc14.jar` o `ojdbc5.jar` esté incluido en el directorio.

Acerca de esta tarea

Los informes importados se configuran inicialmente para utilizar un origen de datos predeterminado. Debe modificar las propiedades de origen de datos de cada informe de TADDM para poder utilizar la base de datos en la que se almacenan los datos de descubrimiento. Los informes de TADDM no utilizan un origen de datos compartido. Por lo tanto, realice los pasos siguientes para configurar las propiedades de los orígenes de datos de todos los informes de TADDM.

Procedimiento

Para configurar orígenes de datos JDBC para Tivoli Common Reporting, complete los siguientes pasos:

1. Si utiliza Tivoli Common Reporting 1.3, complete los siguientes pasos:
   a. En la tabla **Informes** de Tivoli Common Reporting, pulse con el botón derecho del ratón en el informe de TADDM que desea configurar.
   b. Pulse en **Orígenes de datos** en el menú emergente.
   c. En la ventana **Orígenes de datos del informe**, especifique la información del controlador JDBC, del URL, del ID de usuario y de la contraseña. Puede encontrar los valores correctos para estos valores en el archivo `collation.properties` del directorio `$COLLATION_HOME/etc`.
   d. Repita los pasos anteriores para cada uno de los informes de TADDM que desee configurar.
2. Si se utiliza Tivoli Common Reporting 2.1 o 3.1, complete los siguientes pasos:
   a. Abra una línea de mandatos y navegue hasta `tip_install_dir/tip21Components/TCRComponent/bin` para Tivoli Common Reporting 2.1 o hasta `JazzSM_install_dir/reporting/bin` para Tivoli Common Reporting 3.1.
   b. Para configurar todos los orígenes JDBC de todos los informes, ejecute el mandato **`modify`** en una línea:

      Importante: Los mandatos siguientes incluyen el nombre del directorio que contiene informes BIRT, `'IBM Tivoli Products'`. Este nombre se aplica a TADDM 7.3.0.1 y posterior. Si utiliza TADDM 7.3.0, sustituya este nombre por `'Tivoli Products'`.

      ```
      trcmd -user ID_usuario -password contraseña -modify
      -datasources -reports -reportname "/content/package[@name='IBM Tivoli
      Products']/folder[@name='TADDM Reports']//report" -setdatasource
      odaDriverClass=clase_controlador odaURL=url_jdb
      odaUser=usuario_bd odaPassword=contraseña_bd
      ```

      Por ejemplo, si utiliza una base de datos DB2, escriba el mandato siguiente en una línea:

      ```
      trcmd -user tipadmin -password tipadmin -modify -datasources -reports
      -reportname "/content/package[@name='IBM Tivoli Products']/folder[@name=
      'TADDM Reports']//report" -setdatasource
      odaDriverClass=com.ibm.db2.jcc.DB2Driver
      odaURL=jdbc:db2://100.101.102.103:50000/SAMPLEDB
      odaUser=db2inst1 odaPassword=db2inst1
      ```

      Por ejemplo, si utiliza una base de datos Oracle, escriba el mandato siguiente en una línea:

      ```
      trcmd -user tipadmin -password tipadmin -modify -datasources -reports
      -reportname "/content/package[@name='IBM Tivoli Products']/folder[@name=
      'TADDM Reports']//report" -setdatasource
      odaDriverClass=oracle.jdbc.driver.OracleDriver
      odaURL=jdbc:oracle:thin:@192.168.0.1:1521:orcl
      odaUser=taddm_dev odaPassword=taddm_dev
      ```

Verificación de informes de TADDM

Puede comprobar que los informes de TADDM se visualizan correctamente en Tivoli Common Reporting.

Procedimiento

Para verificar que los informes de TADDM se están visualizando correctamente en Tivoli Common Reporting, complete estos pasos:

1. Abra la página de inicio de Tivoli Common Reporting.
2. Pulse **Informes** > **Common Reporting**.
3. Asegúrese de que se muestran las carpetas **TADDM** y **Productos Tivoli**.
4. Pulse en **TADDM**.
5. Pulse en el icono **Ejecutar** para ejecutar uno de los informes. Se visualiza el informe.
6. Asegúrese de que el informe se visualiza completa y correctamente.
7. Utilice la indicación de ruta para regresar a **Carpetas públicas**.
8. Pulse en **Productos Tivoli** > **Informes TADDM**. Pulse en el icono **Ejecutar** para ejecutar uno de los informes. Se visualiza el informe.
9. Asegúrese de que el informe se visualiza completa y correctamente.

Elaboración de informes con BIRT

Puede utilizar la función de informes de Business Intelligence and Reporting Tools (BIRT) para ejecutar informes predefinidos y personalizados basados en los datos de la base de datos de TADDM.

Visión general de los informes de BIRT

Además de los informes incorporados disponibles en el Portal de gestión de datos, también puede diseñar, desarrollar e instalar informes basados en el sistema Business Intelligence and Reporting Tools (BIRT) de código abierto.

Importante: La visualización de informes de BIRT en Data Managemenet Portal en BIRT Report Viewer (motor de tiempo de ejecución BIRT) no es segura, por lo que está inhabilitada. Es preferible ver los informes de BIRT utilizando Tivoli Common Reporting (TCR) después de importar los informes de TADDM a TCR.

Si está al corriente de los riesgos, puede restaurar BIRT Report Viewer y utilizarlo como se especifica en los siguientes párrafos.

TADDM incluye el motor de tiempo de ejecución BIRT de código abierto como un componente integrado. Asimismo, TADDM también incluye cientos de vistas de base de datos predefinidas e informes predefinidos. Además de los informes predefinidos, también puede utilizarse la herramienta del diseñador de BIRT para crear nuevos informes con el fin de utilizar estos con el motor de tiempo de ejecución de BIRT de TADDM. Estos informes pueden utilizar orígenes de datos JDBC que extraen datos mediante la utilización de vistas de base de datos predefinidas.

La interfaz del Portal de gestión de datos proporciona varias formas de gestionar estos informes de BIRT. Puede añadir nuevos informes, descargar informes seleccionados, suprimir informes que ha cargado o ejecutar informes. Los informes predefinidos también están empaquetados para que puedan utilizarse con la herramienta Tivoli Common Reporting.

Business Intelligence and Reporting Tools

Business Intelligence and Reporting Tools (BIRT) es un sistema basado de código abierto en Eclipse que se utiliza para diseñar, desarrollar y ejecutar informes.

Puede desarrollar informes de BIRT para TADDM, y diseñar estos para que utilicen orígenes de datos JDBC y consultas SQL de vistas de base de datos predefinidas.

Importante: Los informes de BIRT no deben utilizar datos tomados directamente de las tablas de base de datos de TADDM. En su lugar, diseñe siempre sus informes para que utilicen un origen de datos JDBC y las vistas de la base de datos de TADDM que se documentan en la *Guía del desarrollador del SDK* de TADDM.

El sistema BIRT incluye dos componentes principales:

- El diseñador BIRT, una herramienta gráfica para diseñar y desarrollar nuevos informes
- El motor de tiempo de ejecución BIRT, que proporciona soporte para ejecutar informes y representar la salida de los informes publicados.

TADDM incluye el motor de tiempo de ejecución de BIRT, que puede utilizar para ejecutar los informes predefinidos. Si desea crear sus propios informes de BIRT, debe descargar la herramienta del diseñador de BIRT que corresponda con la versión del motor de tiempo de ejecución de BIRT incluida con TADDM (actualmente, la versión 2.2.1).

Para obtener más información acerca del proyecto BIRT, lo que incluye cómo descargar la herramienta del diseñador de BIRT, consulte http://www.eclipse.org/birt.

Tareas relacionadas:

"Restauración de BIRT Report Viewer" en la página 195
Si conoce los riesgos relacionados con la seguridad y aún así desea utilizar BIRT Report Viewer, puede restaurarlo.

Informes de BIRT predefinidos

Los informes de BIRT predefinidos que se incluyen con TADDM proporcionan información acerca de los sistemas informáticos, los sistemas operativos y los procesos de servidores que se han descubierto.

Informe de inventario de servidores de aplicaciones:

El informe de inventario de servidores de aplicaciones incluye todos los servidores de aplicaciones descubiertos por TADDM. Cuando se ejecuta el informe, se puede especificar un valor de parámetro para limitar el informe a los servidores de aplicaciones de un tipo específico. El informe agrupa los servidores de aplicaciones descubiertos por sistema, y se muestran por nombre de host completo.

Los datos para este informe se toman de la vista de base de datos CM_APP_SERVERS_PER_HOST_V.

Informe de inventario de sistemas informáticos:

El informe de inventario de sistemas informáticos incluye todos los sistemas informáticos de la base de datos de TADDM que tienen asignadas direcciones IP, listados por el nombre de host completo. Este informe no tiene ningún parámetro.

Este informe se ha diseñado para su exportación a un archivo separado por comas que puede importarse a una aplicación de hoja de cálculo. Si un sistema no tiene dirección IP, este no se incluye en el informe. El mismo sistema informático puede

aparecer varias veces en el informe, una vez por cada dirección IP exclusiva (incluida la dirección de bucle de retorno 127.0.0.1).

Los datos para este informe se toman de la vista de base de datos CM_COMPUTER_SYSTEMS_V.

Informe de inventario de sistemas informáticos por tipo de sistema operativo:

El informe de inventario de sistemas informáticos por tipo de sistema operativo incluye todos los sistemas informáticos descubiertos cuyos sistemas operativos se hayan descubierto también. Este informe no tiene ningún parámetro.

Este informe se ha diseñado para su exportación a un archivo separado por comas que puede importarse a una aplicación de hoja de cálculo. El mismo sistema informático puede aparecer varias veces en el informe, una vez por cada dirección IP exclusiva (incluida la dirección de bucle de retorno 127.0.0.1). Para que pueda incluirse en este informe, un sistema operativo debe estar asociado a un sistema de la base de datos de TADDM. De forma similar, los sistemas que no tienen definido un sistema operativo en la base de datos de TADDM no se incluyen.

Pulse en el nombre de un sistema del informe para que se abra un informe de detalles de inventario de acceso a los detalles detallado para ese sistema.

Los datos para este informe se toman de las vistas de base de datos siguientes:
- DP_UNITARY_COMP_GENERAL_V
- DP_UNITARY_COMP_OS_V
- DP_UNITARY_COMP_IP_INTERFACE_V
- BB_OPERATINGSYSTEM62_V

Informe IP de ITNM:

Proporciona información sobre las instancias instaladas del producto Network Manager y lista todos los recursos de Network Manager que tienen una relación con un sistema informático.

El informe de inventario de Network Manager se encuentra disponible en la consola de TADDM Domain Manager. El informe consta de las secciones siguientes:

Resumen de servidor
Proporciona información sobre las instancias instaladas del producto Network Manager, lo que incluye la versión instalada de Network Manager, las direcciones de host de los servidores donde Network Manager está instalado y los URL para acceder a la GUI de Network Manager.

Resumen de recursos
Lista todos los recursos de Network Manager que tienen una relación con un sistema informático, lo que incluye información sobre su dirección IP, el fabricante, el tipo de recurso (por ejemplo, direccionador) y el identificador exclusivo de la base de datos de Network Manager.

Informe de inventario de sistemas informáticos conciso:

El informe de inventario de sistemas informáticos conciso permite ver las direcciones IP descubiertas mediante el perfil de descubrimiento de Nivel 1. Para cada dirección IP, el informe muestra también el nombre del sistema informático

asociado, así como el nombre del sistema operativo o del software de control (en caso de que se haya descubierto esta información).

Aunque el informe de inventario de sistemas informáticos conciso está concebido para su uso tras un descubrimiento de Nivel 1, puede utilizarse también después de un descubrimiento de Nivel 3. No obstante, otros informes, como el informe de inventario de sistemas informáticos, proporcionan información más detallada tras un descubrimiento con credenciales.

Informe de red de canal de fibra:

El informe de red de canal de fibra muestra conexiones de canal de fibra entre un conmutador de canal de fibra seleccionado y otros sistemas informáticos.

Para ejecutar el informe, especifique el nombre de ámbito mundial (WWN) del conmutador de canal de fibra para ver las conexiones de canal de fibra entre este conmutador y otros sistemas informáticos. En la ventana Parámetro, escriba el nombre (WWN) o selecciónelo de la lista desplegable de conmutadores de canal de fibra descubiertos.

En el informe se visualiza la siguiente información para cada sistema informático conectado:

- Sistema informático (nombre de visualización; WWN en el caso de conmutadores de canal de fibra)
- Fabricante
- Modelo
- Número de serie

Puede pulsar en el nombre de visualización de un sistema informático en el informe para abrir otro informe de red de canal de fibra. Este informe muestra las conexiones de canal de fibra entre el sistema informático seleccionado y otros sistemas informáticos.

Informe de inventario de adaptadores de bus de host:

El informe de inventario de adaptadores de bus de host muestra una lista con todos los adaptadores de bus de host descubiertos y los sistemas informáticos en los que están instalados.

Para cada adaptador de bus de host descubierto, en el informe se visualiza la siguiente información:

Nombre de adaptador de bus de host
El nombre del adaptador de bus de host.

Nombre de dominio completo
El nombre de dominio completo de los sistemas informáticos en los que está instalado el adaptador de bus de host.

El host utiliza matrices de almacenamiento
Un valor booleano que indica si el sistema informático host utiliza volúmenes de almacenamiento ubicados en una matriz de almacenamiento.

Resumen de inventario:

El Resumen de inventario incluye un gráfico circular de los sistemas operativos instalados en los sistemas descubiertos, en función de los ámbitos que TADDM ha

descubierto. Cada segmento del gráfico representa un tipo de sistema operativo e indica el recuento total de servidores descubiertos que ejecutan ese sistema operativo. Este informe no tiene ningún parámetro.

Pulse en cualquier segmento del gráfico para abrir un Informe de inventario de sistemas informáticos detallado para el tipo de sistema operativo seleccionado.

Los datos para este informe se toman de la vista de base de datos BB_OPERATINGSYSTEM62_V.

Informe de cobertura de supervisión:

Los informes de cobertura de supervisión muestran información detallada acerca de los diferentes componentes de su entorno. Puede generar un informe para los sistemas operativos, bases de datos, aplicaciones de Microsoft, servidores VMware y componentes de System p de su entorno. Estos componentes los supervisan los agentes de IBM Tivoli Monitoring 6.1 o posterior. Puede ejecutar este informe desde el panel Informes de BIRT (Business Intelligence and Reporting Tool) del el portal de gestión de datos.

Tabla 37 en la página 183 lista los informes de cobertura disponibles. La cobertura de supervisión de informes para sistemas operativos la puede llenar el sensor de IBM® Tivoli® Monitoring Scope. Sin embargo, los informes restantes requieren que el adaptador de biblioteca de descubrimiento (DLA) de IBM® Tivoli® Monitoring llene los informes.

Los informes contienen tres secciones:

Cobertura por tipo

En esta sección se muestra el número de instancias supervisadas, no supervisadas y totales agrupadas por tipo de informe. La ventana Detalles de cobertura muestra una representación gráfica de las estadísticas siguientes:

- Cobertura total
- Cobertura por plataforma

Detalles de cobertura

Esta sección visualiza el nombre de dominio completo, el nombre del sistema gestionado y el estado de supervisión agrupados por tipo de informe. El estado de supervisión aparece, junto con la información de la versión del agente, si se supervisa. Si se pulsa sobre el MSN de un sistema supervisado, se abre la ventana Detalles de agente.

Detalles de agente

Esta sección muestra información detallada sobre el agente y el sistema operativo que se ejecuta en él. La información visualizada depende de si el agente está supervisado o no. Se incluye información de afinidad y de señal de origen junto con un enlace de iniciación en contexto con la vista de Tivoli Enterprise Portal de IBM Tivoli Monitoring.

La sección Sistema de Software de gestión proporciona un inventario de los agentes de IBM Tivoli Monitoring instalados y un enlace de inicio contextual con espacios de trabajo de IBM Tivoli Monitoring. El Resumen de cobertura de supervisión proporciona una lista de sistemas supervisados y no supervisados, que se puede utilizar para supervisar y mantener agentes de supervisión.

Un descubrimiento de nivel 1 puede utilizar el sensor de IBM Tivoli Monitoring Scope para llenar la cobertura de supervisión para el informe de sistemas operativos. Los otros informes los debe llenar el adaptador de biblioteca de descubrimiento (DLA) de IBM Tivoli Monitoring. Consulte la *Guía del administrador* de TADDM para obtener información sobre el DLA de IBM Tivoli.

Tabla 37 lista los informes de cobertura disponibles.

Tabla 37. Informe de cobertura de supervisión

Nombre del informe	**Descripción**
Cobertura de supervisión para sistemas operativos	Este informe muestra los detalles del sistema operativo de su entorno.
Cobertura de supervisión para bases de datos	Este informe muestra los detalles de la instancia de DB2 y el servidor SQL de su entorno.
Cobertura de supervisión de aplicaciones Microsoft	Este informe muestra los detalles de Active Directory, Cluster Server, Exchange Server, Host Integration Server, el rol habilitado del servidor Hyper-V y el servidor de Internet Information Services.
Cobertura de supervisión para VMware	Este informe muestra los detalles para los servidores de VMware ESX y los servidores de VMware Virtual Center.
Cobertura de supervisión para System p	Este informe muestra los detalles para System p, la consola de gestión de hardware, el servidor de E/S virtual y las particiones lógicas de AIX.

Informes de sensor:

Los informes de sensor predefinidos intercalan la información recopilada sobre métricas de sensor.

El Tabla 38 muestra los informes de sensor predefinidos disponibles.

Tabla 38. Informes de sensor predefinidos

Nombre del informe	**Descripción**
TADDM_SENSORS_WEEKLY_METRICS_ALL TADDM_SENSORS_WEEKLY_METRICS	Este informe muestra el índice de éxito semanal en porcentaje de los sensores que están habilitados en un perfil de descubrimiento de nivel 1, un perfil de descubrimiento de nivel 2 o un perfil de descubrimiento de nivel 3. Se visualiza la siguiente información: • Fecha • % de éxito de Nivel 1 (N1) • % de éxito de Nivel 2 (N2) • % de éxito de Nivel 3 (N3) • % de éxito de N1, N2 • % de éxito de todos El segundo informe "TADDM_SENSORS_WEEKLY_METRICS" contiene la misma información pero presenta dicha información mediante un gráfico de barras.

Tabla 38. Informes de sensor predefinidos (continuación)

Nombre del informe	Descripción
TADDM_SENSORS_SUMMARY_TOTAL TADDM_SENSORS_SUMMARY	Este informe muestra el número total de sensores que se han ejecutado y se han completado correctamente. Se visualiza la siguiente información: • Nivel • Ejecuciones con elementos de configuración almacenados • Éxitos • Anomalías Además, se visualiza un resumen que muestra los niveles de perfil de descubrimiento y las tasas generales de éxito y error en porcentaje correspondientes a cada nivel. El informe "TADDM_SENSORS_SUMMARY" muestra el índice de éxito y de fracaso en porcentaje correspondiente a sensores individuales durante un descubrimiento. Se visualiza la siguiente información: • Nivel • Sensor • Ejecuciones • Éxitos • Anomalías • % de éxito • % de anomalías
TADDM_SENSORS_SERVER_SCANS_IP	Este informe muestra el estado después de explorar un servidor mediante la especificación de la dirección IP. Se visualiza la siguiente información: • Semana • Estado La parte inicial del informe muestra información de resumen sobre la dirección IP, el nombre de host, el nombre de dominio completo, el estado y la fecha de la primera exploración y el estado y la fecha de la última exploración.
TADDM_SENSORS_SERVER_SCANS_ HOSTNAME	Este informe muestra el estado después de explorar un servidor mediante la especificación del nombre de host. Se visualiza la siguiente información: • Semana • Estado La parte inicial del informe muestra información de resumen sobre el nombre de host, la dirección IP, el nombre de dominio completo, el estado y la fecha de la primera exploración y el estado y la fecha de la última exploración.
TADDM_SENSORS_MONTHLY_COVERAGE	Este informe visualiza un gráfico de barras que muestra la cobertura mensual del sensor Sesión. Incluye información sobre el número de exploraciones ejecutadas y el número de exploraciones que han tenido éxito y las que no. El sensor Sesión crea una sesión entre el servidor TADDM y el sistema de destino.

Tabla 38. Informes de sensor predefinidos (continuación)

Nombre del informe	Descripción
TADDM_SENSORS_METRICS_LEVEL_1_ AND_2 TADDM_SENSORS METRICS_LEVEL3	Este informe muestra un gráfico de barras que muestra, para una semana en concreto, el porcentaje de éxito de los sensores individuales en la realización de un descubrimiento de Nivel 1 y Nivel 2. El gráfico de barras correspondiente al informe "TADDM_SENSORS METRICS_LEVEL3" muestra las métricas de los sensores individuales al realizar un descubrimiento de Nivel 3.
TADDM_SENSORS_FAILED_LEVELS_1_2_3 TADDM_SENSORS_FAILED_LEVEL	Este informe muestra un gráfico circular correspondiente a una semana concreta basado en las anomalías en la realización de un descubrimiento de Nivel 1, Nivel 2 o Nivel 3. Cada segmento del gráfico representa problemas de sesión, problemas de sensor, problemas de conexión y otros problemas. El gráfico circular correspondiente al informe "TADDM_SENSORS_FAILED_LEVEL" muestra las métricas de un nivel de descubrimiento especificado.
TADDM_SENSORS_EVENTS_SENSOR_IP TADDM_SENSORS_EVENTS_SENSOR TADDM_SENSORS_EVENTS_IP TADDM_SENSORS_DONE_EVENTS_RUN	Este informe muestra los datos de suceso correspondientes a un sensor y una dirección IP especificados. Se visualiza la siguiente información: • Fecha • Detalles del sensor • Gravedad • Descripción El informe "TADDM_SENSORS_EVENTS_SENSOR" contiene la misma información pero muestra los datos de suceso correspondientes a un sensor en concreto. El informe "TADDM_SENSORS_EVENTS_IP" contiene la misma información pero muestra los datos de suceso correspondientes a una dirección IP especificada. El informe "TADDM_SENSORS_DONE_EVENTS_RUN" contiene la misma información pero muestra los datos de suceso correspondientes a una ejecución de descubrimiento especificada.

Afinidad de servidor por ámbito:

El informe de afinidad de servidor por ámbito muestra relaciones entre servidores, organizadas en función del origen y el destino de cada relación. La primera tabla muestra todos los servidores dentro del ámbito especificado que son orígenes de relaciones y las conexiones desde esos servidores a otros servidores. La segunda tabla muestra todos los servidores dentro del ámbito especificado que son destinos de relaciones, y las conexiones con esos servidores desde otros servidores.

El informe de afinidad de servidor por ámbito solo está disponible en despliegues de servidor de dominio.

Para ver un gráfico que muestre las comunicaciones de servidor a servidor, pulse en **Iniciar el gráfico de afinidades**. El gráfico muestra dependencias transaccionales y de servicio entre sistemas informáticos, y dichas dependencias se indican mediante enlaces trazados entre sistemas. El gráfico incluye todos los

enlaces de dependencias que incluyen al menos un sistema dentro del ámbito de descubrimiento, y los sistemas que son miembros del ámbito están resaltados en amarillo.

Los enlaces mostrados en el gráfico de afinidades pueden representar relaciones transaccionales o de servicio. La dirección de un enlace indica qué sistema es el origen y cual es el destino de la relación de dependencia. Los objetos de origen y de destino pueden ser de varios tipos, en función de la relación:

- Sistema informático
- Servidor de aplicaciones
- Servicio

Los enlaces en el gráfico siempre se trazan entre sistemas informáticos. En el caso de una relación que implique a un servicio o un servidor de aplicaciones, el enlace conecta con el sistema informático host. Para ver más información sobre una relación de dependencia (incluidos el origen, el destino, el nombre de mandato y el número de puerto involucrados), ponga el puntero del ratón sobre el enlace en el diagrama.

El informe de afinidad de servidores por ámbito no se puede importar a Tivoli Common Reporting.

Informes de instantáneas:

Los informes de instantáneas predefinidos intercalar la información capturada por una o más instantáneas.

Una instantánea es una copia de la información del sistema descubierta tomada en un momento específico. Para obtener más información sobre cómo crear instantáneas, consulte “Utilización de la herramienta de instantáneas” en la página 195.

El nombre del informe específico depende del servidor en el que se estén ejecutando y visualizando informes de BIRT. Si está utilizando el portal de gestión de datos en el servidor de dominio o en el servidor de almacenamiento, ejecute el informe estándar, por ejemplo, TADDM_SNAPSHOT_CHANGE. Si se utiliza el portal de gestión de datos en el servidor de sincronización, ejecute el informe con "SYNC" en el nombre, por ejemplo, TADDM_SNAPSHOT_SYNC_CHANGE. Los siguientes informes constituyen excepciones y tienen el mismo nombre en todos los servidores:

- TADDM_SNAPSHOT_FRAME
- TADDM_SNAPSHOT_HOST

Cuando se importa un informe de BIRT a Tivoli Common Reporting, se muestra un nombre de informe cambiado. Por ejemplo, el informe TADDM_SNAPSHOT_SYNC_SESSION_FAILED se visualiza como “TADDM: detalles sobre sesiones fallidas (Enterprise)”.

Tabla 39 en la página 187 muestra los informes de instantánea predefinidos que están disponibles.

Tabla 39. Informes de instantánea predefinidos

Nombre del informe	Descripción
TADDM_SNAPSHOT_FRAME	Visualiza la siguiente información detallada sobre los servidores descubiertos: • nombre de marco • número de serie • fabricante • modelo • tipo de CPU • velocidad de CPU • número de CPU • memoria • ubicación • área de soporte • último descubrimiento
TADDM_SNAPSHOT_HOST	Visualiza la siguiente información detallada sobre servidores físicos y virtuales: • nombre de marco • nombre del sistema • dirección IP • tipo de SO • tipo de host • nombre del sistema gestionado • último descubrimiento
TADDM_SNAPSHOT_SESSION_FAILED TADDM_SNAPSHOT_SYNC_SESSION _FAILED	Visualiza la información del nombre y la dirección IP de los servidores descubiertos sobre los que TADDM no ha podido conseguir información de N2 debido a sesiones fallidas.
TADDM_SNAPSHOT_CHANGE TADDM_SNAPSHOT_SYNC_CHANGE	Compara dos instantáneas tomadas en diferentes momentos. Muestra la siguiente información sobre los servidores que se han añadido o eliminado en el tiempo transcurrido entre las dos instantáneas: • nombre • dirección IP • virtual También muestra información sobre el cambio en la proporción entre servidores físicos y virtuales en el tiempo transcurrido entre las dos instantáneas.
TADDM_SNAPSHOT_DISCOVERY_ERROR TADDM_SNAPSHOT_SYNC _DISCOVERY_ERROR	Muestra información sobre errores generados durante los descubrimientos.
TADDM_SNAPSHOT_FQDN_OS _CHANGES TADDM_SNAPSHOT_SYNC_FQDN _OS_CHANGES	Muestra información sobre los servidores con FQDN (nombres de dominio completos) cambiados, o información sobre sistemas operativos, en el tiempo transcurrido entre dos instantáneas.

Tabla 39. Informes de instantánea predefinidos (continuación)

Nombre del informe	Descripción
TADDM_SNAPSHOT_REFERENCE TADDM_SNAPSHOT_SYNC_REFERENCE	Compara una instantánea con una lista de referencia. Muestra información sobre los servidores que están en la lista de referencia pero no en la instantánea, y sobre los servidores que están en la instantánea pero no en la lista de referencia.
TADDM_SNAPSHOT_RECONCILIATION_SUMMARY TADDM_SNAPSHOT_SYNC_RECONCILIATION_SUMMARY	Le solicita una instantánea y muestra la siguiente información de resumen sobre los servidores descubiertos: • nombre de host de línea base • dirección IP de línea base • nombre de host de TADDM • dirección IP de TADDM • estado • razón del error
TADDM_SNAPSHOT_RECONCILIATION_DETAIL TADDM_SNAPSHOT_SYNC_RECONCILIATION_DETAIL	Le solicita una instantánea y muestra la siguiente información detallada sobre los servidores descubiertos: • nombre de host de línea base • dirección IP de línea base • nombre de host de TADDM • dirección IP de TADDM • estado • razón del error • descripción del error • nombre del ámbito • exclusión filtrada • trama de TADDM • nombre de host de TADDM • FQDN de TADDM • nombre de TADDM • DisplayName de TADDM • JdoClass de TADDM • OsDerived de TADDM • OsName de TADDM • dirección IP de TADDM • número de serie de TADDM • fabricante de TADDM • modelo de TADDM • tipo de host de TADDM • virtual de TADDM • tipo de TADDM • dato de descubrimiento de TADDM

Informe de matrices de almacenamiento por host:

El informe de matrices de almacenamiento por host muestra una lista de los volúmenes de almacenamiento y las matrices de almacenamiento utilizados por un sistema informático especificado.

Al ejecutar un informe, se le solicita que especifique el nombre de host del sistema informático para que el que desea ver información de almacenamiento. En la ventana Parámetro, escriba el nombre de host o selecciónelo de la lista desplegable.

En el informe se visualiza la información siguiente:

- Volumen de almacenamiento
- Matriz de almacenamiento
- Fabricante
- Modelo
- Número de serie
- Capacidad disponible
- Capacidad asignada

Informe de consumidores de matriz de almacenamiento:

El informe de consumidores de matriz de almacenamiento muestra una lista de los sistemas informáticos y los servidores de aplicaciones que utilizan una matriz de almacenamiento especificada.

Al ejecutar un informe, se le solicita que especifique el nombre de una matriz de almacenamiento. En la ventana Parámetro, escriba el nombre de la matriz de almacenamiento o selecciónela de la lista desplegable.

El informe se visualiza con la forma de las tres tablas siguientes:

Sistemas informáticos que utilizan la matriz de almacenamiento *nombre_matriz_almacenamiento*

Estas tabla lista todos los sistemas informáticos descubiertos que utilizan la matriz de almacenamiento especificada.

Servidores de aplicaciones que utilizan la matriz de almacenamiento *nombre_matriz_almacenamiento*

Estas tabla lista todos los servidores de aplicaciones descubiertos que utilizan la matriz de almacenamiento especificada.

Aplicaciones empresariales que utilizan la matriz de almacenamiento *nombre_matriz_almacenamiento*

Esta tabla lista todas las aplicaciones empresariales que utilizan la matriz de almacenamiento especificada.

Informe de topología de conexiones de sistemas:

El informe de topología de conexiones de sistemas muestra un informe textual de los sistemas informáticos con conexiones de redes a sistemas informáticos o desde ellos. Cuando ejecuta un informe, debe introducir el elemento de configuración para el que desea ejecutar el informe, y debe especificar si se trata de un sistema informático o de una aplicación empresarial.

Si el informe se ejecuta para un sistema informático, todos los sistemas informáticos con conexiones de red con el sistema informático seleccionado o

desde este se muestran en una tabla, junto con las métricas de cada conexión de red. Si el informe se ejecuta para una aplicación empresarial, todos los sistemas informáticos con conexiones de red con la aplicación empresarial seleccionada o desde esta se muestran en una tabla.

Puede ver la topología de conexiones de sistemas correspondiente a cada sistema informático pulsando en el nombre del sistema en el informe.

Informe de utilización máxima del sistema por hora:

El informe de utilización máxima del sistema por hora muestra los valores de máxima utilización por hora del sistema en un ámbito y fecha especificados.

Las métricas de utilización incluyen la información siguiente:

- Utilización de la CPU del 95 por ciento por hora
- Utilización de memoria en porcentaje máximo por hora
- Utilización máxima del ancho de banda de red por hora
- Utilización máxima de E/S de disco por hora

Informe de utilización del sistema:

El informe de utilización del sistema muestra la configuración genérica del sistema operativo del servidor y la información de utilización asociada.

Los datos de configuración del sistema operativo del servidor incluyen la información siguiente:

- CPU
- memoria
- sistema de archivos

Esta es la información de configuración del servidor más reciente de la que dispone TADDM. Los datos de utilización del servidor incluyen la siguiente información:

- CPU
- memoria
- red
- disco

Informe de servidores desconocidos:

El informe de servidores desconocidos incluye todos los procesos de servidor descubiertos que TADDM no ha reconocido. El informe agrupa los procesos de servidor descubiertos por sistema, y los muestra por nombre de host completo. Este informe no tiene ningún parámetro.

Los servidores desconocidos se identifican después de que un agente de compilación de topología realice un descubrimiento. El agente de compilación de topología se ejecuta en segundo plano de forma periódica, en función del valor de la frecuencia configurada, por lo que es posible que los servidores desconocidos no se puedan reconocer inmediatamente tras completarse un descubrimiento. Cada cuatro horas es la frecuencia predeterminada con la que se ejecuta el agente de compilación de topología.

Por este motivo, si ejecuta el Informe de servidores desconocidos antes de que el agente de compilación de topología haya finalizado, es posible que el informe no muestre todos los servidores desconocidos.

En el informe se visualiza la información siguiente:

Nombre
El nombre del sistema en el que se está ejecutando el proceso de servidor desconocido.

IP de contexto
La dirección IP del sistema en el que se está ejecutando el proceso de servidor desconocido.

PID El ID de proceso del proceso de servidor desconocido.

PPID El ID de proceso del proceso padre del proceso de servidor desconocido.

Línea de mandatos
El mandato que se utiliza para ejecutar el proceso de servidor desconocido.

Los datos para este informe se toman de la vista de base de datos BB_RUNTIMEPROCESS15_V.

Ejecución de un informe de BIRT

Puede utilizar la sección Analítica del Portal de gestión de datos para ejecutar un informe de BIRT.

Acerca de esta tarea

Importante: La ejecución de un informe de BIRT en Data Management Portal sólo es posible si tiene habilitado BIRT Report Viewer. BIRT Report Viewer está inhabilitado por problemas de seguridad. La forma alternativa de ver los informes de BIRT es utilizando Tivoli Common Reporting (TCR) después de importar los informes de TADDM a TCR. Si está al corriente de los riesgos, puede restaurar BIRT Report Viewer.

Procedimiento

Para ejecutar un informe de BIRT, complete los pasos siguientes:

1. En el panel Funciones, pulse en **Analítica**.
2. En la sección Analítica, pulse en **Informes BIRT**. Se abrirá la lista **Informes BIRT de TADDM**, en la que se mostrarán todos los informes de BIRT disponibles.
3. En la lista **Informes BIRT de TADDM**, realice pulse para resaltar el informe que desea ejecutar.
4. Opcional: Especifique el valor de etiqueta de ubicación. El valor `com.ibm.cdb.locationTaggingEnabled` del archivo `COLLATION_HOME/etc/collation.properties` debe definirse como `true`. Solo se visualizan los datos de informe correspondientes a esta etiqueta de ubicación.

   Nota: Los informes de BIRT incluidos en TADDM actualmente no soportan filtrado de ubicación sin personalización adicional.
5. Pulse en **Ejecutar informe**. Si el informe tiene parámetros, se le solicitará que especifique los valores de dichos parámetros. Cuando haya terminado de especificar los valores de los parámetros, pulse en **Aceptar**.

Resultados

El informe formateado aparece en la ventana del visor de informes de BIRT. Pulse en los iconos de la parte superior del informe para avanzar y retroceder por este, imprimirlo o exportarlo a un archivo. Para abrir un informe de acceso a los detalles que muestre detalles adicionales sobre un subconjunto de los datos del informe, pulse en un enlace del informe.

Nota: Los informes exportados en formato .doc son compatibles con Microsoft Word 2003 o posterior.

Ejecución de un informe de BIRT desde la interfaz de línea de mandatos

Puede ejecutar un informe de BIRT desde la interfaz de línea de mandatos del servidor de TADDM.

Procedimiento

Para ejecutar un informe de BIRT desde la interfaz de línea de mandatos, complete los siguientes pasos:

1. Abra un indicador de mandatos y, en función de la versión del TADDM que utiliza, vaya a uno de los siguientes directorios:
   - 7.3.0: `$COLLATION_HOME/deploy-tomcat/birt-viewer/WEB-INF/resources`
   - 7.3.0.1 y posterior: `$COLLATION_HOME/apps/birt-viewer/WEB-INF/resources`
2. Establezca la variable `BIRT_HOME`. Realice una de las acciones siguientes:
   - En Linux, en función de la versión de TADDM que utiliza, ejecute uno de los siguientes mandatos:
     - 7.3.0:

       ```
       export BIRT_HOME=$COLLATION_HOME/deploy-tomcat/birt-viewer
       ```
     - 7.3.0.1 y posterior:

       ```
       export BIRT_HOME=$COLLATION_HOME/apps/birt-viewer
       ```
   - En Windows, en función de la versión de TADDM que utiliza, ejecute uno de los siguientes mandatos:
     - 7.3.0:

       ```
       set BIRT_HOME=%COLLATION_HOME%/deploy-tomcat/birt-viewer
       ```
     - 7.3.0.1 y posterior:

       ```
       set BIRT_HOME=%COLLATION_HOME%/apps/birt-viewer
       ```
3. Ejecute el informe de BIRT. Realice una de las acciones siguientes:
   - En Linux, ejecute el siguiente mandato:

     ```
     ./genReport.sh -f formato -o salida -F parámetros informe
     ```
   - En Windows, ejecute el siguiente mandato:

     ```
     genReport.bat -f formato -o salida -F parámetros informe
     ```

   Las siguientes opciones de la línea de comandos se utilizan con el programa **genReport**:

   formato
   El formato de salida del archivo de informe. Los valores válidos son PDF y HTML.

   salida La vía de acceso al archivo de informe que desea producir. Por ejemplo, `/home/cognos/utilization.pdf` en Linux, o `C:\data\utilization.pdf` en Windows.

parámetros

(Opcional). La vía de acceso al archivo de propiedades, donde cada propiedad representa un parámetro que el informe necesita. Por ejemplo: `/home/cognos/utilization.properties` en Linux, o `C:\data\utilization.properties` en Windows.

El siguiente texto es un ejemplo de contenido de un archivo de propiedades:

```
scope=All Windows Machines
metric=ALL
operator=N/A
value1=N/A
value2=N/A
appdeps=N/A
```

Debe asegurarse de que los espacios que haya en un nombre de parámetro se evitan mediante el carácter de barra inclinada invertida. Por ejemplo, si el nombre del parámetro es `Snapshot ID Parameter`, la entrada en el archivo de propiedades debería ser

```
Snapshot\ ID\ Parameter=mi_id
```

informe

La vía de acceso al informe que desea ejecutar, con la serie "compiled" añadida al nombre. Por ejemplo:

- En Linux y TADDM 7.3.0: `$COLLATION_HOME/deploy-tomcat/birt-viewer/WEB-INF/report/taddm_server_utilization.rptdesigncompiled`.
- En Linux y TADDM 7.3.0.1 y posterior: `$COLLATION_HOME/apps/birt-viewer/WEB-INF/report/taddm_server_utilization.rptdesigncompiled`.
- En Windows y TADDM 7.3.0: `%COLLATION_HOME%\deploy-tomcat\birt-viewer\WEB-INF\report\taddm_server_utilization.rptdesigncompiled`.
- En Windows y TADDM 7.3.0.1 y posterior: `%COLLATION_HOME%\apps\birt-viewer\WEB-INF\report\taddm_server_utilization.rptdesigncompiled`

Resultados

Nota: El mandato **genReport** no genera informes de acceso a los detalles. Por ello, los enlaces incluidos en el informe generado no funcionan.

Importación de un informe de BIRT

Puede utilizar el portal de gestión de datos para añadir informes personalizados mediante la importación de diseños de informe de BIRT.

Antes de empezar

Para añadir un informe personalizado, primero debe diseñar y desarrollar el informe mediante la utilización de la herramienta del diseñador de BIRT. El diseño de informe debe guardarse en un archivo `.rptdesign` al que pueda acceder desde el sistema cliente.

Nota: Fix Pack 3 En TADDM 7.3.0.3 y posteriores, las columnas de las vistas ampliadas de la base de datos de atributos tienen tipos de datos específicos, como por ejemplo, VARCHAR. En los releases de TADDM anteriores, las columnas solo

tenían el tipo CLOB. Por lo tanto, una vez que actualice a Fix Pack 3, es posible que dejen de funcionar los informes BIRT que utilizan atributos ampliados. Por ejemplo, si las columnas de atributos ampliados no se difunden a un tipo de datos específico, por ejemplo, VARCHAR, puede que se generen errores.

Procedimiento

Para importar un informe de BIRT, complete los siguientes pasos:

1. En el panel Funciones del el portal de gestión de datos, pulse en **Analítica**.
2. En la sección Analítica, pulse en **Informes BIRT**. La lista **Informes BIRT de TADDM** se abre y muestra todos los informes de BIRT disponibles.
3. Pulse **Nuevo**.
4. Cuando se le solicite, especifique los detalles del nuevo informe, incluidos el nombre, la descripción y la ubicación del archivo de diseño de informe. El nombre y la descripción se utilizan para identificar el informe en la lista **Informes BIRT de TADDM**.
5. Pulse en **Aceptar**.

Resultados

El diseño del informe se carga en el servidor y el nuevo informe pasa a estar disponible desde el portal de gestión de datos.

Nota: Si el informe ya existe en el servidor, la importación no se produce. Esto puede suceder incluso si el informe existente no está visible en el portal de gestión de datos. (Por ejemplo, el informe Afinidad de servidor no está soportado en el servidor de sincronización y, por ello, no se muestra en el portal de gestión de datos aunque exista en el servidor).

Supresión de un informe de BIRT

Puede utilizar el portal de gestión de datos para suprimir informes de BIRT del servidor.

Antes de empezar

La supresión de un informe del servidor elimina el archivo `.rptdesign` que el informe utiliza del directorio de informes del servidor. Si desea guardar el diseño del informe para poder utilizarlo en el futuro, asegúrese de contar con una copia de seguridad del archivo `.rptdesign` antes de suprimir el informe.

Procedimiento

Para suprimir un informe de BIRT, complete los pasos siguientes:

1. En el panel Funciones, pulse en **Analítica**.
2. En la sección Analítica, pulse en **Informes BIRT**. La lista **Informes BIRT de TADDM** se abre y muestra todos los informes de BIRT disponibles.
3. Seleccione el informe que desea suprimir.
4. Pulse **Suprimir**.
5. Para renovar la lista **Informes BIRT de TADDM**, pulse en **Renovar**.

Resultados

El informe seleccionado se suprime del servidor y ya no se visualiza en la lista **Informes BIRT de TADDM** del el portal de gestión de datos. Además, el archivo

`.rptdesign` correspondiente al informe se elimina del directorio de informes del servidor de TADDM.

Exportación de un diseño de informe de BIRT

Puede utilizar el Portal de gestión de datos para exportar un diseño de informe de BIRT desde el servidor.

Acerca de esta tarea

Puede que desee exportar un diseño de informe si desea utilizar un informe existente en el que basar un nuevo informe personalizado o si desea importar el diseño del informe a un servidor distinto.

Procedimiento

Para exportar un diseño de informe de BIRT, realice los pasos siguientes:

1. En el panel Funciones, pulse en **Analítica**.
2. En la sección Analítica, pulse en **Informes BIRT**. La lista **Informes BIRT de TADDM** se abre y muestra todos los informes de BIRT disponibles.
3. Seleccione el informe que desee exportar.
4. Pulse en **Descargar**.
5. Cuando el navegador se lo solicite, especifique que desea guardar el archivo y especifique una ubicación.

Resultados

El diseño que utiliza el informe seleccionado se guarda en la ubicación que se ha especificado como un archivo .rptdesign. Puede abrir y modificar este archivo mediante la herramienta del diseñador de BIRT.

Restauración de BIRT Report Viewer

Si conoce los riesgos relacionados con la seguridad y aún así desea utilizar BIRT Report Viewer, puede restaurarlo.

Procedimiento

1. En el archivo `collation.properties`, establezca la propiedad `com.ibm.taddm.birtviewer.enabled` en `true`:

   ```
   com.ibm.taddm.birtviewer.enabled=true
   ```

2. Reinicie el servidor de TADDM.

   Nota: En caso de la actualización del servidor de TADDM, este distintivo está establecido en `false` de forma predeterminada.

Utilización de la herramienta de instantáneas

Puede utilizar la herramienta de instantáneas para realizar una copia de la información del sistema informático, sucesos de descubrimiento y las aplicaciones de servidor en ejecución en el momento de la instantánea.

También puede utilizar la herramienta de instantáneas para cargar información utilizada en el proceso de reconciliación, por ejemplo, para:

- Cargar una lista de servidores esperados, conocida también como lista de referencia.
- Cargar una lista de servidores excluidos.

Puede utilizar informes para consultar la información capturada por la herramienta de instantáneas, por ejemplo:

- Los servidores que se han añadido o eliminado.
- La proporción entre servidores físicos y virtuales.
- Los servidores que no han descubierto completamente debido a que no se ha podido establecer una sesión ssh correctamente.
- El delta entre la lista de servidores descubiertos y la lista de los que se esperaban.

Restricción: Tome instantáneas tras la finalización de la ejecución de los agentes de topología y de descubrimiento. Si toma una instantánea antes de que los agentes de topología terminen de procesar la información descubierta, algunos informes de instantánea, como el Informe de sesión de instantáneas fallida, podrían quedar incompletos.

Sintaxis del mandato snapshot.sh:

Puede utilizar el mandato `snapshot.sh` para tomar una instantánea del sistema y los servidores y sucesos asociados. El mandato `snapshot.sh` se encuentra en el directorio `$COLLATION_HOME/bin`.

Puede ejecutar el mandato `snapshot.sh` en el servidor de TADDM. En un despliegue de servidor de modalidad continua, debe ejecutar el mandato `snapshot.sh` en el servidor de almacenamiento primario.

Sintaxis del mandato

snapshot.sh *acción* [*parámetro_acción*]

Parámetros

addexclude *nombre_archivo* [*lista_exclusión*]
Añade la lista de exclusión al archivo o sustituye una instancia que haya de esta en el archivo.

addref *nombre_archivo* [*lista_referencia*]
Añade la lista de referencia al archivo o sustituye una instancia existente de esta en el archivo.

clear
Borra todos los datos de instantánea y descarta las tablas.

compare [*instantánea_A instantánea_B*]
Muestra el delta entre las dos últimas instantáneas, o la instantánea_A y la instantánea_B, en base al nombre de host.

compareref [*instantánea_A lista_referencia*]
Muestra el delta entre la instantánea y la lista de referencia.

comparesig [*instantánea_A instantánea_B*]
Muestra el delta entre las dos últimas instantáneas, o la instantánea_A y la instantánea_B, en base a la signatura de cambios que hay en el nombre de host o el sistema operativo.

compsys
Muestra los sistemas informáticos.

detail [*instantánea_A*]
Muestra todos los detalles de los sistemas informáticos que haya en la última instantánea o instantánea_A.

detailos [*instantánea_A*]
Muestra la información sobre el sistema operativo de los sistemas informáticos que haya en la última instantánea o instantánea_A.

help
Muestra ayuda detallada sobre el uso del mandato **snapshot.api**.

list [*instantánea_A*]
Muestra la última instantánea o instantánea_A.

listall [*valor_predeterminado*]
Muestra todas las instantáneas.

listexclude [*lista_exclusión*]
Muestra la última lista de exclusión o la que se especifique por su nombre.

listref [*lista_referencia*]
Muestra la última lista de referencia o la que se especifique por su nombre.

listallexclude
Muestra todas las listas de exclusión.

listallref
Muestra todas las listas de referencia.

nosession [*instantánea_A*]
Muestra los sistemas informáticos que han tenido algún error al alojar una sesión en la última instantánea o instantánea_A.

remove *instantánea_A* [*tipo*]
Elimina la instantánea A o elimina todas las instantáneas del tipo que se haya especificado.

removeexclude *lista_exclusión*
Elimina la lista de exclusión especificada por su nombre.

removeref *lista_referencia*
Elimina la lista de referencia especificada por su nombre.

session [*instantánea_A*]
Muestra los sistemas informáticos que han alojado una sesión en la última instantánea o instantánea_A.

sensorerror [*instantánea_A*]
Muestra todos los errores de sensor desde la última instantánea o instantánea_A.

take [*tipo*] [*descripción*]
Toma una instantánea, incluyendo información sobre tipo y descripción, si se especifica.

Utilización de la herramienta de instantáneas como ayuda para reducir el número de servidores físicos:

Puede utilizar la herramienta de instantáneas al sustituir muchos servidores físicos por menos servidores físicos mediante la ejecución de servidores virtuales.

Procedimiento

Para obtener información útil al intentar reducir el número de servidores físicos utilizados, complete los pasos siguientes:

1. Realice un descubrimiento de todos los sistemas conocidos.
2. Utilización de la herramienta de instantáneas, tomar una instantánea.

   ```
   snapshot.sh take
   ```

   De forma opcional, puede añadir a la instantánea información sobre tipo y descripción:

   ```
   snapshot.sh take tipo descripción
   ```
3. En el Portal de gestión de datos, ejecute el informe TADDM_SNAPSHOT_SESSION_FAILED. El informe devuelve información sobre los sistemas que no se han descubierto porque no se pudo establecer una sesión ssh.
4. Asegúrese de que pueden establecerse sesiones ssh en todos los sistemas. Es posible que sea necesario actualizar los detalles de autenticación de TADDM.
5. Realice un descubrimiento de solo los sistemas a los que no se ha accedido como parte del primer descubrimiento para asegurarse de que todas los problemas de conexión se han resuelto.
6. Tras algún periodo de tiempo, por ejemplo, un mes, realice un descubrimiento de todos los sistemas conocidos.
7. En el Portal de gestión de datos, ejecute el informe TADDM_SNAPSHOT_CHANGE. El informe devuelve información sobre los sistemas nuevos visibles desde que se tomara la instantánea, los sistemas que ya no están presentes y la proporción entre servidores físicos y virtuales en porcentajes.

Utilización de la herramienta de instantáneas para reconciliar listas de sistemas esperados y reales:

Puede utilizar la herramienta de instantáneas y los informes predefinidos para verificar que la lista de servidores disponibles en la red coincide con la lista de servidores esperados.

Procedimiento

Para reconciliar los sistemas reales y esperados, complete los pasos siguientes:

1. Prepare una lista de referencia que contenga la lista de servidores esperados. La lista de referencia es un archivo de texto con formato de valores separados por comas (CSV) y con los campos siguientes:
   - nombre de host
   - dirección IP
   - trama
   - sistema operativo
   - tipo de host
   - comentarios
   - área de soporte
   - ubicación

   Para obtener más información sobre la sintaxis del archivo de referencia, ejecute el mandato **snapshot.sh** con el parámetro de ayuda:

   ```
   snapshot.sh help
   ```

2. Si es necesario, prepare una lista de exclusión que contenga la lista de servidores que se deben ignorar en el proceso de reconciliación. La lista de exclusión es un archivo de texto con formato CSV que contiene los campos siguientes:
   - nombre de host
   - tipo de exclusión

   Para obtener más información sobre la sintaxis del archivo de exclusión, ejecute el mandato **snapshot.sh** con el parámetro de ayuda:

   ```
   snapshot.sh help
   ```
3. Utilización de la herramienta de instantáneas, tomar una instantánea.

   ```
   snapshot.sh take
   ```

   De forma opcional, puede añadir a la instantánea información sobre tipo y descripción:

   ```
   snapshot take tipo descripción
   ```
4. En el Portal de gestión de datos, ejecute uno de los siguientes informes de BIRT:
   - TADDM_SNAPSHOT_RECONCILIATION_SUMMARY
   - TADDM_SNAPSHOT_RECONCILIATION_DETAIL

Utilización de informes de instantánea en un despliegue de servidor de sincronización:

Puede recopilar información en un despliegue de servidor de sincronización mediante la ejecución de la versión de empresa de los informes de instantánea predefinidos.

Procedimiento

Para ejecutar informes de instantáneas predefinidos en un despliegue de servidor de sincronización, complete los pasos siguientes:

1. Si aún no se ha creado, configure la tabla de instantáneas. Para ello, realice los pasos siguientes:
   a. En cada servidor TADDM, ejecute el mandato `snapshot.sh` sin parámetros.
   b. Reinicie TADDM en cada dominio y servidor de sincronización.

   Este procedimiento crea las tablas de instantáneas si es que aún no existen. Solo es necesario configurar las tablas de instantánea una única vez por cada entorno TADDM.
2. Ejecute un descubrimiento en cada dominio de TADDM y tome una instantánea en cada dominio cuando sea necesario.
3. Realice una sincronización en el servidor de sincronización. Asegúrese de incluir todos los dominios.
4. Cree una instantánea de empresa. En el servidor de sincronización, ejecute el siguiente mandato:

   ```
   snapshot.sh take
   ```
5. Ejecute los informes en cada dominio. Utilice la versión normal de cada informe de instantánea, por ejemplo, `TADDM_SNAPSHOT_CHANGE`.
6. Ejecute los informes en el servidor de sincronización. Utilice la versión de empresa de cada informe de instantánea, por ejemplo, `TADDM_SNAPSHOT_SYNC_CHANGE`.

Integración de TADDM con otros productos Tivoli

Para disponer de más prestaciones a la hora de gestionar su entorno de TI, puede integrar IBM Tivoli Application Dependency Discovery Manager (TADDM) con otros productos Tivoli, incluyendo IBM Tivoli Business Service Manager, IBM Tivoli Monitoring, y los sistemas de gestión de sucesos como IBM Tivoli Netcool/OMNIbus.

Versiones soportadas

Puede utilizar la siguiente tabla para ver qué versiones de los productos con los que TADDM se puede integrar están soportadas.

La siguiente tabla muestra las versiones soportadas de los productos con los que TADDM se puede integrar.

Tabla 40. Las versiones soportadas de los productos.

Nombre de producto	Versión soportada
Servicio de menú contextual y servicio de integración de datos (CMS/DIS)	
IBM Control Desk (ICD)	• 7.6
IBM SmartCloud Control Desk (SCCD)	• 7.5.1 - Utilice el último nivel de fixpack disponible
IBM Tivoli Business Service Manager (TBSM)	• 4.2.1 - Utilice el último nivel de fixpack disponible • 6.1.0 - Utilice el último nivel de fixpack disponible • 6.1.1 - Utilice el último nivel de fixpack disponible
IBM Tivoli Change And Configuration Management Database (CCMDB)	• 7.2.1
IBM Tivoli Integration Composer (ITIC)	• 7.5.1 - Utilice el último nivel de fixpack disponible
IBM Tivoli Monitoring (ITM)	• 6.2.1 • 6.2.2 - FP3 • 6.2.3 • 6.3
IBM Tivoli Netcool/OMNIbus	• 7.3 • 7.4 • Fix Pack 1 8.*x* - soportado con TADDM 7.3.0.1 y posterior
IBM Tivoli Network Manager IP (ITNMIP)	• 3.9 • 4.1
Jazz for Service Management (JazzSM)	• 1.1
Tivoli Common Reporting (TCR)	• 1.3 • 2.1.1 • 3.1

Tabla 40. Las versiones soportadas de los productos. (continuación)

Nombre de producto	Versión soportada
Tivoli Directory Integrator (TDI)	• 7.0 • 7.1 • 7.1.1
Tivoli Netcool/IMPACT	• 7.1
Tivoli Workload Scheduler (TWS)	• 1.5.1 • 8.6

Para obtener más información sobre los productos que se integran con TADDM, consulte su documentación:

- Para obtener información sobre el Servicio de menú contextual y servicio de integración de datos (CMS/DIS), consulte el tema *Configuración del servicio de menú contextual y servicio de integración de datos* en la *Guía de instalación* de TADDM.
- IBM Control Desk (ICD)
- IBM SmartCloud Control Desk (SCCD)
- IBM Tivoli Business Service Manager (TBSM)
- IBM Tivoli Change and Configuration Management Database (CCMDB)
- IBM Tivoli Integration Composer (ITIC)
- IBM Tivoli Monitoring (ITM)
- IBM Tivoli Netcool/OMNIbus
- IBM Tivoli Network Manager IP (ITNMIP)
- Jazz for Service Management (JazzSM)
- Tivoli Common Reporting (TCR)
- Tivoli Directory Integrator (TDI)
- Tivoli Netcool/Impact
- Tivoli Workload Scheduler (TWS)

Integración de TADDM con IBM Tivoli Monitoring mediante la automatización de OSLC

Se puede integrar TADDM con IBM Tivoli Monitoring utilizando la automatización de OSLC. Si desea integrar TADDM con IBM Tivoli Monitoring 6.3, es aconsejable utilizar la automatización de OSLC. El método antiguo de la integración con el uso del sensor de IBM Tivoli Monitoring Scope está en desuso y se eliminará en los próximos releases.

TADDM utiliza la infraestructura de IBM Tivoli Monitoring de dos formas:

- TADDM obtiene la lista de puntos finales de IBM Tivoli Monitoring de Tivoli Enterprise Portal Server mediante la sesión de automatización de OSLC.
- TADDM ejecuta mandatos CLI en los sistemas de destino para los sensores en los descubrimientos de nivel 2 y 3 y captura la salida de dichos mandatos.

Si tiene algún problema, consulte el tema *Problemas del proveedor de servicios de automatización de ejecución de OSLC de ITM* en la *Guía de resolución de problemas* de TADDM.

Fix Pack 5

Requisitos previos:

Si utiliza Windows 7 o posterior, necesitará:

1. PowerShell versión 2+
2. URL SOAP TEMS
3. Compruebe que se puede conectar tanto a TEMS como a TEPS.

En la siguiente tabla se proporcionan unos pasos que debe llevar a cabo para habilitar correctamente la integración de TADDM con IBM Tivoli Monitoring mediante la automatización de OSLC.

Tabla 41. Integración de TADDM con IBM Tivoli Monitoring mediante la automatización de OSLC

Paso	Detalles
Configuración de los hosts de ITM Tivoli Enterprise Monitoring Server (TEMS) e ITM TEPS	"Configuración de los hosts de ITM Tivoli Enterprise Monitoring Server (TEMS) e ITM TEPS" en la página 206
Instalación del proveedor de servicios de automatización de ejecución de OSLC en IBM Tivoli Monitoring **Nota:** Asegúrese de que cumple todos los requisitos previos especificados en "Requisitos previos para la instalación del proveedor de servicios de automatización de ejecución de OSLC en IBM Tivoli Monitoring" en la página 206.	"Instalación del proveedor de servicios de automatización de ejecución de OSLC en IBM Tivoli Monitoring" en la página 209
Configuración de TADDM para utilizar el proveedor de servicio de automatización de ejecución de OSLC	"Configuración de TADDM para utilizar el proveedor de servicio de automatización de ejecución de OSLC" en la página 214
Configure TADDM para el descubrimiento: • Configure las propiedades de automatización en el archivo `collation.properties`. • Cree una nueva entrada de lista de acceso del tipo `<"Integration">"OSLC Automation"` en la lista de acceso.	"Configuración del descubrimiento mediante la sesión de automatización de OSLC" en la página 116

Después de completar estos pasos puede ejecutar un descubrimiento utilizando el proveedor de servicios de automatización de ejecución de OSLC de ITM.

Conceptos relacionados:

"Integración de TADDM con otros productos mediante la automatización de OSLC" en la página 213
TADDM puede integrarse con otros productos utilizando la automatización de OSLC (Open Services for Lifecycle Collaboration). TADDM se conecta al proveedor de servicios de automatización de ejecución de OSLC que proporciona datos sobre la infraestructura de otros productos, que pueden descubrirse en TADDM utilizando la sesión de automatización de OSLC.

Proveedor de servicios de automatización de ejecución de OSLC de ITM

El proveedor de servicios de automatización de ejecución de OSCL de ITM se utiliza para importar datos sobre las direcciones IP de los puntos finales

gestionados por IBM Tivoli Monitoring a TADDM y descubrir puntos finales de IBM Tivoli Monitoring mediante la sesión de automatización de OSLC.

La Figura 1. ilustra el TADDM conectado al proveedor de servicios de automatización de ejecución de OSLC de ITM que recopila los datos sobre la infraestructura gestionada por ITM utilizando mandatos KT1.

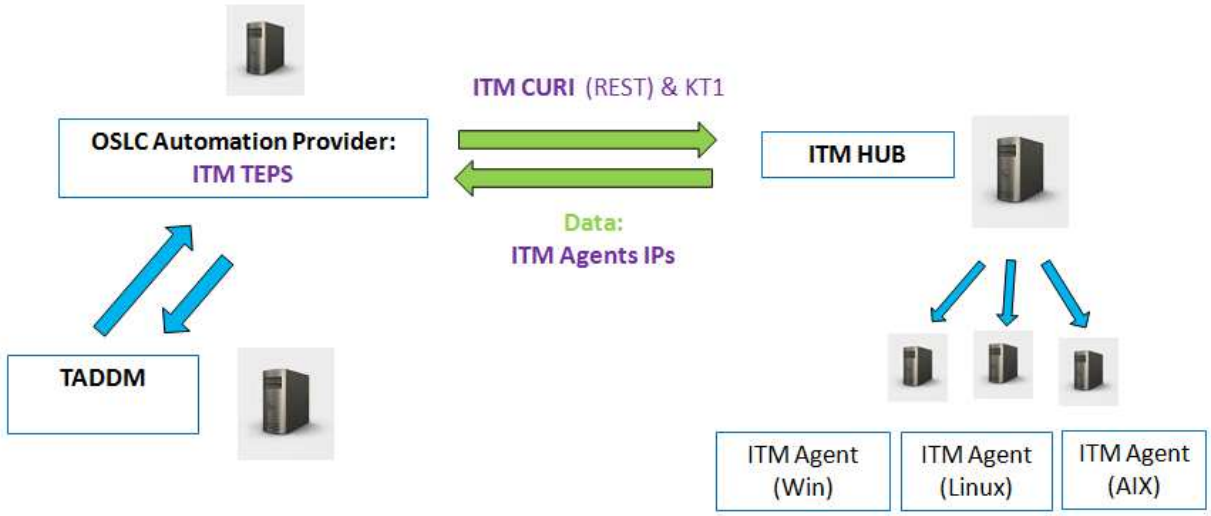

Figura 4. TADDM conectado al proveedor de servicios de automatización de ejecución de OSLC de ITM que recopila los datos sobre la infraestructura gestionada por ITM utilizando mandatos KT1.

TADDM obtiene el destino del proveedor de servicios de automatización de ejecución de OSLC de ITM en los servicios de registro de JAZZ SM o en el archivo `collation.properties`. La Figura 2. ilustra el TADDM que utiliza los servicios de registro de JAZZ SM para obtener la dirección del proveedor de servicios de automatización de ejecución de OSLC.

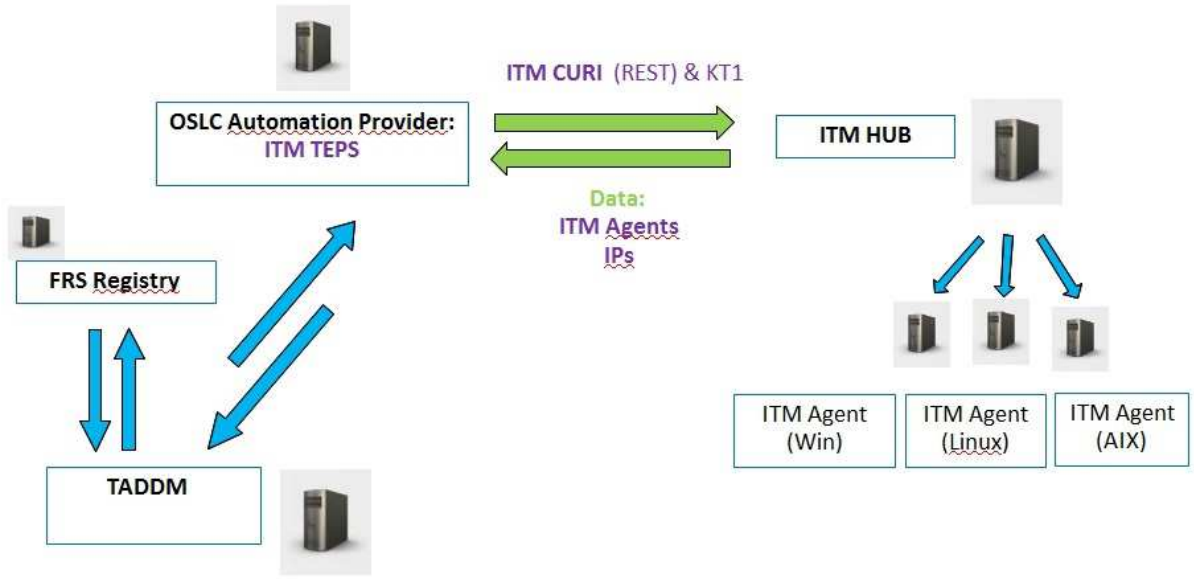

Figura 5. TADDM que utiliza los servicios de registro de JAZZ SM para obtener la dirección del proveedor de servicios de automatización de ejecución de OSLC.

TADDM puede conectarse directamente a varios proveedores de servicios de automatización de ejecución de OSLC y un único servicio de registro de JAZZ SM, donde pueden registrarse varios proveedores. La Figura 3. ilustra las direcciones de descarga de TADDM de los proveedores de servicios de automatización de ejecución de OSLC desplegados en varios ITM TEPS (servidores de portal) desde los servicios de registro de JAZZ SM.

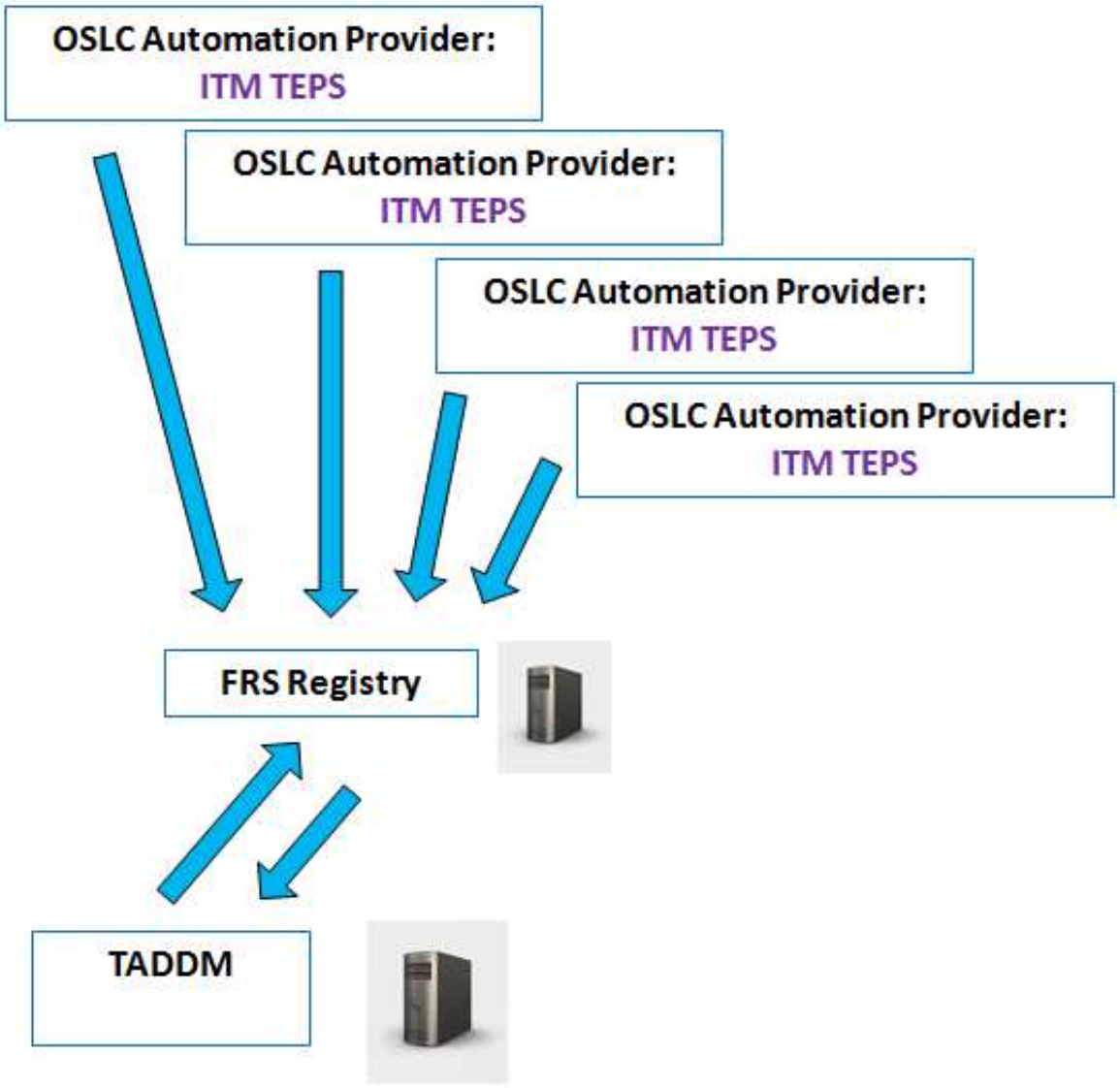

Figura 6. Direcciones de descarga de TADDM de los proveedores de servicios de automatización de ejecución de OSLC desplegados en varios ITM TEPS (servidores de portal) desde los servicios de registro de JAZZ SM.

Conceptos relacionados:

"Proveedor de servicios de automatización de ejecución de OSLC" en la página 213
El proveedor de servicios de automatización de ejecución de OSLC se utiliza para rellenar datos sobre las direcciones IP de los puntos finales gestionados por otros productos en TADDM. Los datos se utiliza para el descubrimiento de puntos finales utilizando la sesión de automatización de OSLC.

Instalación del proveedor de servicios de automatización de ejecución de OSLC de ITM

Para importar datos sobre las direcciones IP de los puntos finales gestionados por IBM Tivoli Monitoring (ITM) a TADDM, o bien para ejecutar un descubrimiento, debe instalar el proveedor de servicios de automatización de ejecución de OSLC en IBM Tivoli Monitoring.

Si tiene algún problema, consulte el tema *Problemas del proveedor de servicios de automatización de ejecución de OSLC de ITM* en la *Guía de resolución de problemas* de TADDM.

Requisitos previos para la instalación del proveedor de servicios de automatización de ejecución de OSLC en IBM Tivoli Monitoring:

Antes de instalar el proveedor de servicios de automatización de ejecución de OSLC en IBM Tivoli Monitoring (ITM) debe configurar el entorno para que cumpla todos los requisitos previos.

El proveedor de servicios de automatización de ejecución de OSLC de ITM debe estar instalado en el host de ITM Tivoli Enterprise Portal Server (TEPS). La versión soportada de IBM Tivoli Monitoring es IBM Tivoli Monitoring 6.3.

Configuración de los hosts de ITM Tivoli Enterprise Monitoring Server (TEMS) e ITM TEPS

Fix Pack 5 **Paso 1- Reconfiguración de TEMS y TEPS**

La mejor forma de realizar la configuración de TEMS y TEPS es utilizar la GUI de Manage Tivoli Enterprise Monitoring Services (MTEMS).

Para el SO Windows, inicie el proceso de ITM **kinconfig .exe** para iniciar la GUI de Manage Tivoli Enterprise Monitoring Services (MTEMS).

Para Unix/Linux, puede iniciar la GUI de MTEMS mediante el mandato de CLO "**./itmcmd manage**".

Para cada uno de los dos componentes de ITM (TEMS y TEPS):

- Resalte el componente en la GUI de MTEMS.
- Pulse con el botón derecho y seleccione Reconfigurar.

Se abrirá la ventana de configuración de TEMS o TEPS.

Proporcione correctamente todos los parámetros de TEMS (Tipo de TEMS, Nombre de TEMS y protocolo en los valores de configuración principales y Nombre de host/Dirección IP y Puerto en los Valores avanzados) y seleccione "**Aceptar**".

Seleccione "**Habilitar el proveedor de datos del panel de control**" en la ventana de configuración de TEPS.

Fix Pack 5 **Paso 2 - Ejecución de scripts de TADDM y configuración**

Este paso incluye la ejecución de dos scripts principales de TADDM para ayudar a configurar la integración de TADDM a ITM.

1. Configure el archivo provider.properties

Host de ITM TEMS

Habilite los mandatos KT1 (**tacmd get/put/execute**) ejecutando uno de los siguientes scripts en el host de ITM TEMS:

- Para sistemas operativos Linux:

```
TADDM_CD_ISO/itm-discovery-support/configure_tems.sh <-i <ITM_HOME>>
 [-t <TEMP-DIR>
```

- Para sistemas operativos Windows:

```
TADDM_CD_ISO/itm-discovery-support/configure_tems.ps1 <-i <ITM_HOME>>
 [-t <TEMP-DIR>
```

donde *<ITM_HOME>* es el directorio de instalación de ITM TEPS, por ejemplo, `/opt/IBM/ITM`, y *<TEMP-DIR>* es el directorio de destino de los archivos temporales. El valor predeterminado del parámetro *<TEMP-DIR>* es `/var/log/automation_provider`.

Fix Pack 5 Cuando haya finalizado, debería ver las líneas siguientes al final de la ejecución del script.

```
INFO: Stopping ITM TEPS...
INFO: ITM TEPS has stopped.
INFO: Starting ITM TEPS...
INFO: ITM TEPS has started.
INFO: Checking if TEPS is running...
INFO: Checking if OSLC Automation Provider is installed...
INFO: Installation of OSLC Automation Provider successfully finished.
```

Nota: Para una validación de id usuario inicial (**tacmd get/put/execute**), utilice **http:1920** o **https:3661** y, a continuación, **ip.pipe:1920** o **ip.spipe:3660** para el trabajo KT1 de un proveedor de automatización para el destino descubierto. Estos protocolos deben habilitarse en ITM para completar el descubrimiento.

Host de ITM TEPS

Verifique si el proveedor de datos del panel de control de ITM está instalado o habilitado. Si no lo está, instálelo o habilítelo de manera opcional. Consulte el tema Verificar que el proveedor de datos del panel de control está habilitado en la documentación de IBM Tivoli Monitoring.

Importante: Si utiliza el sistema operativo Windows de 64 bits, asegúrese de que la VÍA DE ACCESO del sistema (o la entrada de vía de acceso del archivo `kfwenv`) apunta al directorio TMAITM6 de 64 bits. Si no está ahí, añádalo manualmente. Por ejemplo, si tiene instalado ITM en el directorio `C:\IBM\ITM\`, debe tener especificado `C:\IBM\ITM\TMAITM6_x64` en la variable de entorno de la vía de acceso del sistema o en la directiva PATH del archivo `C:\IBM\ITM\CNPS\kfwenv`.

Fix Pack 5

2. Ejecute el script `automation_provider` en el host de ITM TEPS

Ejecute el script **`automation_provider`** en su servidor:

- Para el sistema operativo Linux:

  ```
  automation_provider.sh install  -t /tmp/log  -i /opt/IBM/ITM -c
  /tmp/provider.properties
  ```

- Para el sistema operativo Windows:

  ```
  automation_provider.ps1 install  -t /tmp/log  -i /opt/IBM/ITM -c
  /tmp/provider.properties
  ```

Un punto importante a tener en cuenta es que, aunque se cree un archivo provider.properties antes de ejecutar el script automation_provider, éste se ignorará y se creará un archivo provider.properties "predeterminado" en la vía de acceso de configuración de ITM TEPS ($ITM_HOME/iw/profiles/ITMProfile/installedApps/ITMCell/itmautomationprovider.ear/itmautomationprovider.war/WEB-INF/provider.properties)

Deberá ubicar este archivo, realizar manualmente los cambios correspondientes en los parámetros y, a continuación, reiniciar TEPS para que el archivo sea efectivo.

Archivos requeridos

Los siguientes archivos deben estar presentes en el directorio desde el que ejecuta el script de instalación:

- El script de instalación:
  - Para sistemas operativos Linux y AIX: `TADDM_CD_ISO/itm-discovery-support/automation_provider.sh` y sus submódulos ubicados en `TADDM_CD_ISO/itm-discovery-support/mod/sh/`.
  - Para los sistemas operativos Windows: `TADDM_CD_ISO/itm-discovery-support/automation_provider.ps1` y sus submódulos ubicados en `TADDM_CD_ISO/itm-discovery-support/mod/ps/`.
- `itmautomationprovider.ear`: el paquete con el proveedor de servicios de automatización de ejecución de OSLC de ITM. La ubicación exacta del archivo es `TADDM_CD_ISO/itm-discovery-support/ear/itmautomationprovider.ear`.
- `provider.properties`: el archivo de configuración de ejemplo del proveedor de servicios de automatización de ejecución de OSLC de ITM. El archivo puede configurarse manualmente y pasarse al script de instalación como un parámetro. Si no se pasa, debe proporcionar los parámetros necesarios durante la instalación. La ubicación exacta del archivo es `TADDM_CD_ISO/itm-discovery-support/template_provider.properties`.
- Las bibliotecas de soporte de KT1 para el sistema operativo correspondiente y su arquitectura de 32 o 64 bits.
  - Para sistemas operativos Linux:

    ```
    TADDM_CD_ISO/itm-discovery-support/linux32
    TADDM_CD_ISO/itm-discovery-support/linux64
    ```

  - Para sistemas operativos AIX:

    ```
    TADDM_CD_ISO/itm-discovery-support/aix32
    TADDM_CD_ISO/itm-discovery-support/aix64
    ```

  - Para Linux en IBM System Z (zLinux):

    ```
    TADDM_CD_ISO/itm-discovery-support/linuxz32
    TADDM_CD_ISO/itm-discovery-support/linuxz64
    ```

  - Para sistemas operativos Windows:

    ```
    TADDM_CD_ISO/itm-discovery-support/win32
    TADDM_CD_ISO/itm-discovery-support/win64
    ```

Configuración del archivo `provider.properties`

Opcionalmente, puede configurar el archivo `provider.properties` estableciendo los parámetros siguientes:

- `com.ibm.automationprovider.registration.host=`*`http://localhost:15210`* - habilitar la conexión en ITM. El valor especifica un URL público para TEPS. El valor predeterminado de este parámetro es `http://localhost:15210`.

  Nota: Modifique el host local para representar el nombre de host o la dirección IP del servidor TEPS.
- `com.ibm.automationprovider.itm.curi.url=`*`http://localhost:15210`* - especifica la dirección URL del proveedor de ITM CURI (REST). El valor predeterminado es `http://localhost:15210`.

  Nota: En este caso, modifique el host local o la dirección IP del servidor TEPS.
- `com.ibm.automationprovider.itm.soap.url=`*`http://localhost:1920///cms/soap`* - especifica la dirección URL de ITM SOAP. El valor predeterminado ese `http://localhost:1920///cms/soap`.

Nota: En este caso, modifique el host local para representar el nombre de host o la dirección IP del servidor TEMS del hub, que puede o no estar en el mismo host que el TEPS (la mayoría de los entornos de producción deben tener TEMS y TEPS en servidores diferentes).

Nota: Si tiene una configuración no predeterminada de ITM CURI o ITM SOAP, o si ha configurado la seguridad de SSL en ITM TEPS, o ambos, asegúrese de especificar las direcciones URL correctas para las propiedades `com.ibm.automationprovider.itm.curi.url` y `com.ibm.automationprovider.itm.soap.url`.

Los valores de los parámetros especificados en el archivo `provider.properties` tienen prioridad sobre los valores de los parámetros definidos en la línea de mandatos.

Fix Pack 5 Si tiene intención de ejecutar un descubrimiento en RTEMS, asegúrese de tener el parámetro "`KT1_TEMS_SECURE=YES`" habilitado en el archivo de entorno.

Registro de los proveedores de servicios de automatización de ejecución de OSLC en los servicios de registro de Jazz SM (FRS)

De manera opcional, puede registrar los proveedores de servicios de automatización de ejecución de OSLC en los servicios de registro de Jazz SM. Seleccione uno de los métodos siguientes:

- Añada los parámetros siguientes al archivo `provider.properties`:
  - `com.ibm.automationprovider.frs.url`: especifica la dirección URL de FRS para el registro del proveedor de servicios de automatización de ejecución de OSLC. Se necesita la dirección URL completa de la colección, por ejemplo, `http://9.122.100.100:9083/oslc/pr/collection`.
  - `com.ibm.automationprovider.frs.user`: especifica el nombre de usuario que se utiliza para la conexión a FRS.
  - `com.ibm.automationprovider.frs.password`: especifica la contraseña que se utiliza para la conexión a FRS.
  - `com.ibm.automationprovider.registration.initialdelay=5000`: especifica el tiempo transcurrido entre el inicio del proveedor de servicios de automatización de ejecución de OSLC y el primer intento de registro en FRS. El valor predeterminado es `5000` y se expresa en milisegundos. Para inhabilitar el registro, establezca el valor en `-1`.
- Añada la opción `-f` en la línea de mandatos, por ejemplo, `./automation_provider.sh -f` y, durante la instalación del proveedor, cuando se le solicite, especifique los parámetros necesarios.

Instalación del proveedor de servicios de automatización de ejecución de OSLC en IBM Tivoli Monitoring:

Para instalar el proveedor de servicios de automatización de ejecución de OSLC en IBM Tivoli Monitoring (ITM) debe ejecutar el script `automation_provider`. El proveedor de servicios de automatización de ejecución de OSLC puede instalarse en modalidad interactiva o no interactiva.

Procedimiento

Para instalar el proveedor de servicios de automatización de ejecución de OSLC, ejecute el siguiente script `automation_provider` desde el host de ITM TEPS:

- Para sistemas operativos Linux:

  ```
  TADDM_CD_ISO/itm-discovery-support/automation_provider.sh install
  [-i <ITM-HOME>] [-t <TEMP-DIR>] [[-c <CONFIG-FILE> | [-h <TEPS-IP>]
   [-p <TEPS-PORT>]] [-f]
  ```

- Para sistemas operativos Windows:

  ```
  TADDM_CD_ISO/itm-discovery-support/automation_provider.ps1 install
  [-i <ITM-HOME>] [-t <TEMP-DIR>] [[-c <CONFIG-FILE> | [-h <TEPS-IP>]
   [-p <TEPS-PORT>]] [-f]
  ```

donde:

-i <*ITM-HOME*>
: es el directorio de instalación de ITM TEPS, por ejemplo, `/opt/IBM/ITM`.

-t <*TEMP-DIR*>
: es el directorio de destino de los archivos temporales. El valor predeterminado es `/var/log/automation_provider`.

-h <*TEPS-IP*>
: es la dirección IP del host de ITM TEPS.

-p <*TEPS-PORT*>
: es el puerto HTTP de ITM TEPS.

-c <*CONFIG-FILE*>
: es el destino del archivo `provider.properties`, que contiene la configuración del proveedor de servicios de automatización de ejecución de OSLC.

-f
: es un distintivo que puede utilizar para que se le solicite durante la instalación que proporcione los parámetros necesarios para registrar los proveedores de servicios de automatización de ejecución de OSLC en los servicios de registro de JAZZ SM.

Importante: Todos los parámetros del script de instalación son opcionales. Puede especificarlos en el orden que desee.
Ejemplos:

```
automation_provider.sh install -t /tmp/log -i /opt/IBM/ITM -h 9.100.100.200 -p 15210
automation_provider.ps1 install -i /opt/IBM/ITM
```

- Puede instalar el proveedor de servicios de automatización de ejecución de OSLC en modalidad no interactiva. Efectúe los pasos siguientes:
  1. Configure el archivo `provider.properties`. Consulte la sección "Configuración del archivo provider.properties" en la página 208.
  2. Ejecute el siguiente script `automation_provider` en el host de ITM TEPS:
     - Para sistemas operativos Linux:

       ```
       automation_provider.sh install  -t /tmp/log
       -i /opt/IBM/ITM -c /tmp/provider.properties
       ```

     - Para sistemas operativos Windows:

       ```
       automation_provider.ps1 install  -t /tmp/log
       -i /opt/IBM/ITM -c /tmp/provider.properties
       ```

     Nota: Si tiene una configuración no predeterminada de ITM CURI o ITM SOAP, o si ha configurado la seguridad de SSL en ITM TEPS, o ambos, instale el proveedor de servicios de automatización de ejecución de OSLC en modalidad no interactiva. Asegúrese de especificar las direcciones URL correctas para las propiedades `com.ibm.automationprovider.itm.curi.url` y `com.ibm.automationprovider.itm.soap.url`.

- Puede instalar el proveedor de servicios de automatización de ejecución de OSLC en modalidad interactiva. Durante la instalación, proporcione valores para los parámetros necesarios, tal como se especifica en la sección "Configuración del archivo provider.properties" en la página 208.

Verificación de la instalación del proveedor de servicios de automatización de ejecución de OSLC:

Puede verificar si el proveedor de servicios de automatización de ejecución de OSLC se ha instalado correctamente en IBM Tivoli Monitoring.

Procedimiento

1. Asegúrese de que ITM TEMS esté ejecutando agentes de Windows, Linux o UX. Para ello, ejecute los mandatos siguientes:

   ```
   /opt/IBM/ITM /bin/tacmd login -u admin -p password -s localhost
   /opt/IBM/ITM /bin/tacmd listSystems
   ```

2. Asegúrese de que cada ITM TEMS tenga un plan de automatización. El planes deben contener direcciones IP de puntos finales ITM. Abra las siguientes direcciones web en el navegador web:

   ```
   http://<ITM_TEPS>:<ITM_PORT>/itmautomationprovider
   http://<ITM_TEPS>:<ITM_PORT>/itmautomationprovider/services/plans
   ```

   Ejemplo

   ```
   http://9.100.200.100:15210/itmautomationprovider/services/plans
   ```

Comprobación del estado del proveedor de servicios de automatización de ejecución de OSLC de ITM:

Puede comprobar el estado de la instalación del proveedor de servicios de automatización de ejecución de OSLC de ITM.

Procedimiento

Ejecute el siguiente script `automation_provider`:

- Para el sistema operativo Linux:

  ```
  automation_provider.sh status [i- <ITM-HOME>] [t- <TEMP-DIR>]
  ```

- Para el sistema operativo Windows:

  ```
  automation_provider.ps1 status [i- <ITM-HOME>] [t- <TEMP-DIR>]
  ```

donde:

i- *<ITM-HOME>*
: es el directorio de instalación de ITM TEPS, por ejemplo, `/opt/IBM/ITM`.

t- *<TEMP-DIR>*
: es el directorio de destino de los archivos temporales. El valor predeterminado es `/var/log/automation_provider`.

Importante: Todos los parámetros del script son opcionales. Puede especificarlos en el orden que desee.

Ejemplos

```
automation_provider.sh status
automation_provider.ps1 status -i /opt/IBM/ITM
automation_provider.sh status -t /tmp/log -i /opt/IBM/ITM
```

Desinstalación del proveedor de servicios de automatización de ejecución de OSLC:

Puede desinstalar el proveedor de servicios de automatización de ejecución de OSLC de ITM ejecutando el script `automation_provider`.

Procedimiento

Ejecute el siguiente script `automation_provider`:

- Para el sistema operativo Linux:

  `automation_provider.sh uninstall [i- <ITM-HOME>] [t- <TEMP-DIR>]`

- Para el sistema operativo Windows:

  `automation_provider.ps1 uninstall [i- <ITM-HOME>] [t- <TEMP-DIR>]`

donde:

i- <*ITM-HOME*>
: es el directorio de instalación de ITM TEPS, por ejemplo, `/opt/IBM/ITM`.

t- <*TEMP-DIR*>
: es el directorio de destino de los archivos temporales. El valor predeterminado es `/var/log/automation_provider`.

Importante: Todos los parámetros del script son opcionales. Puede especificarlos en el orden que desee.

Ejemplos

```
automation_provider.sh uninstall
automation_provider.ps1 uninstall -i /opt/IBM/ITM
automation_provider.sh uninstall -t /tmp/log -i /opt/IBM/ITM
```

Configuración del descubrimiento del proveedor de servicios de automatización de ejecución de OSLC de ITM

Cuando utiliza el proveedor de servicios de automatización de ejecución de OSLC de ITM, puede configurar el proceso de descubrimiento ajustando las siguientes propiedades.

com.collation.discover.dwcount=32
: El valor predeterminado es `32`.

  Esta propiedad es una propiedad de servidor TADDM, que define el número de hebras Worker del descubrimiento.

  Para obtener los mejores resultados, defina las propiedades `com.collation.discover.dwcount` and `KT1_RPC_THREADS` en el mismo valor.

com.ibm.automationprovider.kt1.concurenttasks.limit=100
: El valor predeterminado es `100`.

  Esta propiedad es una propiedad de ITM OSLC Execute Automation Service Provider que se puede editar en el archivo `provider.properties`. Define el número de solicitudes simultáneas que el proveedor envía a TEMS. Si hay demasiadas solicitudes, se ponen en cola a nivel del proveedor.

  Nota: Modifique el valor de esta propiedad únicamente si hace malta una mayor regulación entre TADDM y TEMS, o si se definen más de 100 hebras Worker KT1.

KT1_RPC_THREADS=10
: El valor predeterminado es `10`.

Es una propiedad de ITM TEMS que se puede modificar en el archivo `ITM_HOME/config/kbbenv.ini`. Define el número de hebras Worker que responden a solicitudes KT1.

Para obtener los mejores resultados, defina las propiedades `KT1_RPC_THREADS` y `com.collation.discover.dwcount` con el mismo valor.

Integración de TADDM con otros productos mediante la automatización de OSLC

TADDM puede integrarse con otros productos utilizando la automatización de OSLC (Open Services for Lifecycle Collaboration). TADDM se conecta al proveedor de servicios de automatización de ejecución de OSLC que proporciona datos sobre la infraestructura de otros productos, que pueden descubrirse en TADDM utilizando la sesión de automatización de OSLC.

El descubrimiento con el uso del proveedor de servicios de automatización de ejecución de OSLC es un proceso genérico, que puede mejorarse para incluir el descubrimiento de otros productos que implementan sus propios proveedores de servicio de automatización de ejecución de OSLC. Durante el descubrimiento, se abre un puerto por host del proveedor de servicios de automatización de ejecución de OSLC o servicios de registro de Jazz SM, o ambos. Esto garantiza un mejor control de seguridad.

En la tabla siguiente se enumeran los temas que contienen más información sobre el descubrimiento a través de OSLC.

Tabla 42. Temas que contienen más información sobre el descubrimiento a través de OSLC.

Información	**Ubicación**
Configuración del descubrimiento	"Configuración del descubrimiento mediante la sesión de automatización de OSLC" en la página 116
propiedades del servidor de TADDM	"Propiedades para el descubrimiento utilizando la sesión de automatización de OSLC" en la página 86
Sensores que dan soporte al descubrimiento utilizando la sesión de automatización de OSLC	Consulte el tema *Sensores que dan soporte al descubrimiento utilizando la sesión de automatización de OSLC* en la *Referencia de sensores* de TADDM

Proveedor de servicios de automatización de ejecución de OSLC

El proveedor de servicios de automatización de ejecución de OSLC se utiliza para rellenar datos sobre las direcciones IP de los puntos finales gestionados por otros productos en TADDM. Los datos se utiliza para el descubrimiento de puntos finales utilizando la sesión de automatización de OSLC.

TADDM puede obtener el destino del proveedor de servicios de automatización de ejecución de OSLC de ITM en los servicios de registro de Jazz SM o en el archivo `collation.properties`.

TADDM puede conectarse directamente a varios proveedores de servicios de automatización de ejecución de OSLC y una única instancia de servicios de registro de Jazz SM, donde pueden registrarse varios proveedores de servicios de automatización de ejecución de OSLC. Cada proveedor de servicios de

automatización de ejecución de OSLC almacena información sobre una instancia de un determinado producto con el que se integra TADDM, por ejemplo, sobre ITM HUB.

Referencia relacionada:

"Proveedor de servicios de automatización de ejecución de OSLC de ITM" en la página 202
El proveedor de servicios de automatización de ejecución de OSCL de ITM se utiliza para importar datos sobre las direcciones IP de los puntos finales gestionados por IBM Tivoli Monitoring a TADDM y descubrir puntos finales de IBM Tivoli Monitoring mediante la sesión de automatización de OSLC.

Configuración de TADDM para utilizar el proveedor de servicio de automatización de ejecución de OSLC:

Para poder ejecutar el descubrimiento utilizando la sesión de automatización de OSLC, debe configurar TADDM para que utilice el proveedor de servicios de automatización de ejecución de OSLC.

Procedimiento

Para configurar TADDM para que utilice el proveedor de servicio de automatización de ejecución de OSLC, siga estos pasos:

1. Asegúrese de que el proveedor de servicios de automatización de ejecución de OSLC esté instalado y en ejecución.
2. Conectar TADDM al proveedor de servicios de automatización de ejecución de OSLC. Puede hacerlo de dos formas: directamente o utilizando los servicios de registro de Jazz for Service Management. Estos métodos pueden combinarse si hay más de un proveedor de servicios de automatización de ejecución de OSLC.
   - Para conectar directamente TADDM al proveedor de servicios de automatización de ejecución de OSLC, añada las direcciones de los proveedores de servicio de automatización de ejecución de OSLC a la propiedad `com.ibm.cdb.topobuilder.integration.oslc.automationprovider` en el archivo `collation.properties`.
   - Para conectar TADDM al proveedor de servicios de automatización de ejecución de OSLC utilizando los servicios de registro de Jazz for Service Management, habilite la búsqueda de proveedores de servicio de automatización de ejecución de OSLC en los servicios de registro de Jazz for Service Management. Efectúe los pasos siguientes:
     a. Asegúrese de que los servicios de registro de JAZZ SM estén ejecutándose.
     b. Asegúrese de que los proveedores de servicios de automatización de ejecución de OSLC estén conectados a los servicios de registro de Jazz SM.
     c. Configure una de las siguientes propiedades en el archivo `collation.properties` para proporcionar la dirección a los servicios de registro de Jazz SM:

        ```
        com.ibm.cdb.topobuilder.integration.oslc.frsurl
        com.ibm.cdb.topobuilder.integration.oslc.automation.frsurl
        ```
3. Reinicie el servidor de TADDM.

Resultados

Después de configurar TADDM, puede ejecutar el descubrimiento utilizando la sesión de automatización de OSLC.

Referencia relacionada:

"Propiedades para el descubrimiento utilizando la sesión de automatización de OSLC" en la página 86
Estas propiedades se aplican al descubrimiento utilizando la sesión de automatización de OSLC.

Interfaz de línea de mandatos para OSLCAutomationAgent

OSLCAutomationAgent se utiliza para recopilar datos de los proveedores de servicios de automatización de ejecución de OSLC. Puede utilizar mandatos para ejecutar el agente manualmente y para renovar o actualizar los conjuntos de ámbitos que crea.

Las direcciones de los proveedores de servicios de automatización de ejecución de OSLC se configuran en el archivo `collation.properties` o se descargan de los servicios de registro de Jazz SM, o ambos. El agente se conecta a cada proveedor de servicios de automatización de ejecución de OSLC para obtener la lista de planes de automatización compatibles con TADDM. Los planes de automatización están formados por las direcciones IP que el agente utiliza para guardar en la memoria caché y crear los conjuntos de ámbitos de descubrimiento. Por ejemplo, cuando TADDM se integra con IBM Tivoli Monitoring, los planes de automatización están formados por las direcciones IP de los servidores y puntos finales (agentes) de ITM TEMS, que están gestionados por IBM Tivoli Monitoring. OSLCAutomationAgent almacena en caché y crea conjuntos de ámbitos con las direcciones IP de los agentes de IBM Tivoli Monitoring. Cada ITM TEMS tiene un conjunto de ámbitos diferente.

OSLCAutomationAgent se ejecuta periódicamente en el grupo de los agentes de integración.

Puede utilizar los siguientes mandatos en OSLCAutomationAgent.

- Para ejecutar el agente manualmente, utilice el siguiente mandato:

  ```
  /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent
  ```

- Para renovar los conjuntos de ámbitos, utilice el siguiente mandato:

  ```
  /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent -s true
  ```

  Nota: Los conjuntos de ámbitos sólo se renuevan si hay cambios en el plan de automatización del proveedor de automatización de ITM. Para forzar la renovación de los conjuntos de ámbitos, utilice el siguiente mandato:

  ```
  /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent
  --forceScopeSetRefresh true
  ```

  Los conjuntos de ámbitos están disponibles en la consola de Discovery Management en el panel **Ámbitos**.

- Para visualizar los conjuntos de ámbitos en la memoria caché, utilice los siguientes mandatos:

  ```
  /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent -d true
  /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent
   --displayCache true
  ```

  Los conjuntos de ámbitos se visualizan en los siguientes archivos de registro de TADDM:

- <COLLATION_HOME>/dist/log/services/TopologyBuilder.log
- <COLLATION_HOME>/dist/log/agents/OSLCAutomationAgent.log

El siguiente ejemplo muestra la salida que se puede encontrar en el archivo <COLLATION_HOME>/dist/log/agents/OSLCAutomationAgent.log:

```
2014-07-22 11:42:54,660 TopologyBuilder [pool-1-thread-1]  DEBUG
oslc.OSLCAutomationAgent - OSLCAutomationAgent:displaying cache
2014-07-22 11:42:54,669 TopologyBuilder [pool-1-thread-1]  INFO
 oslc.OSLCAutomationAgent - <AGENT_IP_2> http://9.120.100.100:15210/
itmautomationprovider/services/plans/2 1406009933764
2014-07-22 11:42:54,669 TopologyBuilder [pool-1-thread-1]  INFO
 oslc.OSLCAutomationAgent - <AGENT_IP_2> http:///9.120.100.100:15210/
itmautomationprovider/services/plans/2 1406009933764
2014-07-22 11:42:54,675 TopologyBuilder [pool-1-thread-1]  DEBUG
 oslc.OSLCAutomationAgent - OSLCAutomationAgent:cache end
```

Conceptos relacionados:

"Visión general del proceso de compilación de topologías" en la página 16
TADDM ejecuta el proceso de construcción de topología de forma periódica. Hasta que se completa el proceso de compilación de topologías después del descubrimiento o después del funcionamiento de carga en bloque, pueden existir objetos sin reconciliar en la base de datos de TADDM y las relaciones de las topologías pueden estar incompletas.

Integración de TADDM con IBM Tivoli Monitoring (método antiguo)

En función de las tareas específicas que deba llevar a cabo en su entorno de TI, puede utilizar las funciones de integración disponibles entre IBM Tivoli Application Dependency Discovery Manager (TADDM) e IBM Tivoli Monitoring. Puede integrar TADDM con IBM Tivoli Monitoring mediante el sensor de IBM Tivoli Monitoring Scope.

Nuevo método de integración

Importante: A partir de la versión 7.3.0 de TADDM se recomienda efectuar la integración con IBM Tivoli Monitoring 6.3 mediante la automatización de OSLC. El método antiguo de la integración con el uso del sensor de IBM Tivoli Monitoring Scope está en desuso y se eliminará en los próximos releases.

Puede encontrar más información sobre la integración de TADDM con IBM Tivoli Monitoring mediante la automatización de OSLC en "Integración de TADDM con IBM Tivoli Monitoring mediante la automatización de OSLC" en la página 201 y sobre los sensores que admiten el descubrimiento mediante la automatización de OSLC en el tema *Sensores que admiten el descubrimiento mediante la automatización de OSLC* de la *Referencia de sensores* de TADDM.

Método de integración antiguo

Las siguientes secciones hacen referencia al método antiguo de la integración. Puede seguir utilizándolo, pero debe recordar que dicho método está en desuso y se eliminará en los próximos releases.

En la Tabla 1. se correlacionan algunas tareas que es posible que deba efectuar con las prestaciones de integración que debe utilizar, mientras que el resto de las secciones proporcionan una visión general de dichas prestaciones.

Tabla 43. Tareas de usuario con la función de integración correspondiente que debe utilizarse

Tarea	Posibilidades de integración que utilizar
Comprenda mejor cómo funciona la disponibilidad observando los valores del sistema operativo, los valores de aplicación y el historial de cambios de los sistemas que IBM Tivoli Monitoring supervisa.	• "Descubrimiento mediante IBM Tivoli Monitoring" • "Iniciar en contexto" en la página 219
Asegúrese de que se supervise la disponibilidad de los sistemas operativos descubiertos por TADDM.	• "Descubrimiento mediante IBM Tivoli Monitoring" • "Informe de cobertura de supervisión" en la página 219
Ver la disponibilidad y el rendimiento de los sistemas que TADDM ha descubierto.	• "DLA de IBM Tivoli Monitoring" en la página 218 • "Informe de cobertura de supervisión" en la página 219
Supervisar una aplicación de negocio en busca de cambios en la configuración.	• "Descubrimiento mediante IBM Tivoli Monitoring" • "Sucesos de cambio" en la página 219 • "Iniciar en contexto" en la página 219

Descubrimiento mediante IBM Tivoli Monitoring

TADDM puede realizar descubrimientos de nivel 1, nivel 2 y algunos de nivel 3 mediante la infraestructura deIBM Tivoli Monitoring 6.2.1 o posterior. TADDM descubre los elementos de configuración del entorno de IBM Tivoli Monitoring utilizando solamente las credenciales de Tivoli Enterprise Portal Server, en lugar de las credenciales de cada sistema que el servidor de portales supervisa.

TADDM saca el máximo rendimiento de la infraestructura de Tivoli Monitoring en los modos siguientes:

- TADDM obtiene la lista de puntos finales de Tivoli desde Tivoli Enterprise Portal Server para crear información de descubrimiento de nivel 1 y para crear ámbitos de descubrimiento de nivel 2 y 3 más profundos.
- TADDM utiliza la infraestructura de Tivoli Monitoring para ejecutar mandatos CLI en sistemas de destino para los sensores en los descubrimientos de nivel 2 y 3 y para captura la salida de dichos mandatos.

Esta función proporciona las ventajas siguientes:

- Un rápido despliegue de TADDM en los entornos existentes de Tivoli Monitoring.
- No es necesario que exista ningún servidor de pasarela ni ancla TADDM.
- No es necesario definir conjuntos de ámbitos que contengan los sistemas que se deban explorar. Sólo se necesita un ámbito con una única entrada para Tivoli Enterprise Portal Server.
- No es necesario definir ninguna lista de acceso (credenciales de sistema operativo) para los destinos de descubrimiento.
- Sólo se necesita una lista de acceso para el inicio de sesión de la GUI de Tivoli Enterprise Portal Server.

Tabla 44. Temas que incluyen más información sobre el descubrimiento mediante IBM Tivoli Monitoring

Información	Ubicación de la información
Configuración del descubrimiento mediante IBM Tivoli Monitoring	"Configuración del descubrimiento mediante IBM Tivoli Monitoring (método antiguo)" en la página 114
Propiedades del servidor TADDM que se aplican al descubrimiento mediante IBM Tivoli Monitoring	"Propiedades del descubrimiento mediante IBM Tivoli Monitoring (método antiguo)" en la página 84
• Sensores que dan soporte al descubrimiento mediante IBM Tivoli Monitoring • Sensor IBM Tivoli Monitoring Scope, incluida la información acerca de la configuración del sensor y acerca de la resolución de los problemas que pueden producirse durante el despliegue o el uso del sensor.	*Referencia de sensores* de TADDM

DLA de IBM Tivoli Monitoring

El adaptador de biblioteca de descubrimiento (DLA) de IBM Tivoli Monitoring extrae datos de configuración de Tivoli Monitoring sobre los sistemas informáticos y las bases de datos que Tivoli Monitoring supervisa. La salida del DLA es un archivo con formato XML que contiene estos componentes y sus relaciones. La salida del DLA también incluye datos que representan los datos y agentes de Tivoli Monitoring que se utilizan para iniciar las vistas de disponibilidad de TADDM. Para obtener información detallada sobre cómo cargar datos exportados por DLA en TADDM, consulte el tema *El programa de carga masiva* en la *Guía del usuario* de TADDM.

Para ejecutar el DLA, realice los pasos siguientes:

1. Genere el DLA en ITM como se especifica en el tema *Utilización del adaptador de biblioteca de descubrimiento de Tivoli Management Services* en http://www-01.ibm.com/support/knowledgecenter/SSTFXA_6.2.2.1/com.ibm.itm.doc_6.2.2fp1/discoverylibraryadapter_tms.htm?lang=en.
2. Copie el archivo de salida del DLA en el host de TADDM.
3. Utilice el programa de carga masiva para cargar el DLA desde ITM en TADDM. Utilice el mandato siguiente:

   ```
   $COLLATION_HOME/bin/loadidml.sh -u usuario -p contraseña -f vía_al_DLA
   ```

Cuando instala nuevos agentes de Tivoli Monitoring, éstos pueden proporcionar soporte adicional para el DLA de Tivoli Monitoring. Los agentes proporcionan información para cumplimentar los informes de cobertura de supervisión, solamente la cobertura de supervisión de los informes de sistemas operativos no requiere un DLA.

Cuando instala un agente, debe habilitar el soporte de aplicación para estos agentes para así asegurarse de que el agente participa en la salida generada por el DLA. No todos los agentes admiten Tivoli Monitoring DLA.

Para obtener información acerca de cómo configurar el soporte de aplicaciones para los agentes no estándar, consulte la documentación correspondiente. Para

verificar que un agente da soporte al DLA de Tivoli Monitoring, consulte la documentación para el agente de IBM Tivoli Composite Application Manager.

Informe de cobertura de supervisión

Los informes de cobertura de supervisión muestran información detallada acerca de los diferentes componentes de su entorno. Puede generar un informe para los sistemas operativos, bases de datos, aplicaciones de Microsoft, servidores VMware y componentes de System p de su entorno. Estos componentes los supervisan los agentes de IBM Tivoli Monitoring 6.1 o superior.

Para obtener más información sobre los informes de Cobertura de supervisión, consulte la *Guía del usuario* de TADDM .

Sucesos de cambio

Puede configurar TADDM para que notifique a IBM Tivoli Monitoring que se ha detectado un cambio en un recurso descubierto.

Tabla 45. Temas que contienen más información acerca de los sucesos de cambio

Información	Ubicación de la información
• Configuración de TADDM para enviar eventos de cambio • Configuración de un proveedor de datos de IBM Tivoli Monitoring • Configuración de los sucesos de cambio para un sistema empresarial	"Envío de sucesos de cambio a sistemas externos" en la página 228

Iniciar en contexto

Al iniciar en contexto, puede ver los datos de TADDM dentro de las vistas de Tivoli Enterprise Portal de IBM Tivoli Monitoring.

Al configurar las vistas de topología para que aparezcan en Tivoli Enterprise Portal, puede ver las infraestructuras físicas, la infraestructura de la aplicación y las topologías del sistema empresarial dentro de las vistas de disponibilidad de Tivoli Enterprise Portal.

Tabla 46. Temas que contienen más información sobre el inicio en contexto

Información	Ubicación de la información
Los URL que se requieren para poder visualizar las vistas de topología	"Configuración para iniciar en contexto" en la página 225
Instrucciones para configurar el inicio en contexto para poder ver los valores del sistema operativo, los valores de aplicación y el historial de cambios para los sucesos de cambio entrantes.	"Creación de enlaces de detalles los informes de sucesos de cambios de la configuración en IBM Tivoli Monitoring" en la página 239

Registro de elementos de configuración para el servicio de menú contextual y el servicio de integración de datos

Si utiliza el servicio de menú contextual (CMS) y el servicio de integración de datos(DIS) para habilitar puntos de lanzamiento entre productos flexibles, debe registrar los elementos de configuración (CI) de TADDM en la base de datos de CMS/DIS.

Antes de empezar

Antes de utilizar el servicio del menú contextual y el servicio de integración de datos, primero debe configurar la base de datos de CMS/DIS.

Acerca de esta tarea

Los elementos de configuración de TADDM están registrados en la base de datos de CMS/DIS de dos modos:

- Registro inicial mediante el script de registro de CMS/DIS
- Actualizaciones automáticas periódicas realizadas por el agente del compilador de topologías CMSDISAgent

Ejecución del registro inicial

Para completar el registro inicial de los elementos de configuración de TADDM en la base de datos del servicio del menú contextual y del servicio de integración de datos, debe ejecutar manualmente el script **run_cms_dis_registration**. El agente compilador de topologías CMSDISAgent no actualiza automáticamente el registro del elemento de configuración hasta después de haberse completado el registro inicial.

Acerca de esta tarea

Si utiliza el despliegue del servidor de modalidad continua, ejecute el script de registro en el servidor de almacenamiento primario. Si utiliza el despliegue del servidor de sincronización, ejecute el script de registro en el servidor de sincronización.

Procedimiento

Para completar el registro inicial de los elementos de configuración de TADDM:

1. En el indicador de mandatos, navegue hasta el directorio `$COLLATION_HOME/bin`.
2. Ejecute el script **run_cms_dis_registration** para su sistema operativo:
   - Sistemas Linux y UNIX:

     ```
     ./run_cms_dis_registration.sh [ register [identificador exclusivo global] |
                                     clean [identificador exclusivo global [tipo de clase]] |
                                     re-register-all | register-menu |
                                     help ]
     ```

   - Sistemas Windows:

     ```
     run_cms_dis_registration.bat [ register [identificador exclusivo global] |
                                    clean [identificador exclusivo global [tipo de clase]] |
                                    re-register-all | register-menu |
                                    help ]
     ```

   Donde:

   register [*identificador exclusivo global***]**

Registro de datos de TADDM en el servicio de menú contextual y el servicio de integración de datos. Opcionalmente, puede especificar el identificador exclusivo global (GUID) de un objeto de modelo que desee registrar.

La primera vez que ejecute un script con la opción `register` y no haya un identificador exclusivo global especificado, todos los datos de TADDM se registrarán en la base de datos y se registrarán todos los puntos de lanzamiento con el servicio de menú contextual. Ejecuciones posteriores con esta opción sólo registran los cambios en los datos de TADDM que se han producido desde la última ejecución. Esta opción es la opción predeterminada.

Si especifica un identificador exclusivo global, sólo se registra el objeto de modelo con el identificador exclusivo global especificado.

Nota: El registro inicial de todos los datos de TADDM puede tardar más tiempo.

clean [*identificadorExclusivoGlobal* **[***tipoClase***]]**

Anula el registro de los datos de TADDM existentes actualmente en la base de datos.

Si no especifica un identificador exclusivo global, se anulará el registro de todos los datos de TADDM. Si especifica un identificador exclusivo global, sólo se anula el registro del objeto de modelo con el identificador exclusivo global especificado. Si el objeto de modelo con el identificador exclusivo global especificado, ya no está disponible en TADDM, también debe especificar el tipo de objeto de modelo.

re-register-all
Anula el registro de todos los datos de TADDM y lanza puntos, a continuación, repite el registro inicial. Esta opción es equivalente a ejecutar el script con la opción `clean` y, a continuación, con la opción `register`.

register-menu
Actualiza únicamente las definiciones de menú que estén registradas en la base de datos del servicio del menú contextual. Utilice esta opción si los datos de TADDM están registrados pero desea actualizar únicamente las definiciones de menú.

help
Muestra información de ayuda para el script.

Ejemplo

- Este ejemplo registra todos los datos de TADDM con el servicio de menú contextual y el servicio de integración de datos al ejecutarlo por primera vez; en ejecuciones posteriores, registra todos los cambios desde la última ejecución:

  ```
  ./run_cms_dis_registration.sh
  ```

- Este ejemplo registra sólo el objeto de modelo con el identificador exclusivo global especificado.

  ```
  ./run_cms_dis_registration.sh register 3950DF835FA0337A829D864415CC1384
  ```

- Este ejemplo elimina todos los datos de TADDM registrados:

  ```
  ./run_cms_dis_registration.sh clean
  ```

- Este ejemplo elimina el objeto con el identificador exclusivo global especificado y el tipo de objeto del modelo:

```
./run_cms_dis_registration.sh clean 3950DF835FA0337A829D864415CC1384
  LinuxUnitaryComputerSystem
```

- Este ejemplo elimina todos los datos de TADDM registrados y, a continuación, repite el registro:

  ```
  ./run_cms_dis_registration.sh re-register-all
  ```

Qué hacer a continuación

Si desea ejecutar un script de registro de nuevo más adelante, primero debe inhabilitar el agente compilador de topologías CMSDISAgent para detener las actualizaciones incrementales. Para habilitar el agente, edite el archivo `$COLLATION_HOME/etc/collation.properties` y defina la siguiente propiedad:

```
com.ibm.cdb.DisCmsIntegration.enabled=false
```

Cuando el script finaliza, debe volver a habilitar el agente definiendo la propiedad en `true`.

Configuración de CMSDISAgent

CMSDISAgent se ejecuta periódicamente como agente compilador de topologías y actualiza el registro de los elementos de configuración en la base de datos del servicio de menú contextual y del servicio de integración de datos, registrando cualquier elemento de configuración nuevo o modificado y anulando el registro de cualquier elemento de configuración suprimido.

Acerca de esta tarea

Si está habilitado, CMDDISAgent comienza a ejecutarse después de haber completado el registro inicial de los elementos de configuración de TADDM mediante el script **run_cms_dis_registration**. Puede modificar la configuración del agente para cambiar el modo en el que se ejecuta el agente.

Procedimiento

- Para habilitar o inhabilitar CMSDISAgent, edite el archivo `$COLLATION_HOME/etc/collation.properties` y defina la siguiente propiedad:

  ```
  com.ibm.cdb.DisCmsIntegration.enabled=valor
  ```

  donde *valor* es `true` o `false`. Si el valor se define en `true`, el agente se ejecuta periódicamente después de haberse completado el registro inicial. (Esta propiedad no afecta al funcionamiento del script **run_cms_dis_registration**, que se puede ejecutar en cualquier momento.)
- Para personalizar cuáles son los elementos configurables que se registran en la base de datos, modifique los siguientes archivos en el directorio `$COLLATION_HOME/etc/cmsdis`:

  classtype-changehistory.list
  : Lista los tipos de elementos configurables de los objetos del modelo para los que TADDM ha lanzado soporte de iniciación en contexto para el informe del historial de cambios.

  classtype-detailPanel.list
  : Lista los tipos de elementos configurables de los objetos del modelo para los que TADDM ha lanzado soporte de iniciación en contexto para el panel de detalles.

  Puede eliminar los tipos de objetos del modelo que no son necesarios para que otros productos lancen TADDM en contexto. No añada ningún tipo de estos

archivos; puede que TADDM no soporte el lanzamiento en contexto para tipos adicionales. Después de modificar los archivos de la lista de tipo de clase, inhabilite el agente y, a continuación, ejecute de nuevo el script **run_cms_dis_registration**, especificando la opción `re-register-all`.

Creación de un almacén de biblioteca de descubrimiento

Un almacén de biblioteca de descubrimiento es un directorio o carpeta de un sistema del centro de datos y representa la ubicación común donde todos los Adaptadores de biblioteca de descubrimiento (DLA) graban los archivos XML que contienen información de recursos. Los archivos de datos XML que deben cargarse de forma masiva en un sistema TADDM, se colocan en el almacén de biblioteca de descubrimiento. Para utilizar el programa del cargador masivo, debe crear un almacén de biblioteca de descubrimiento.

Antes de empezar

Un DLA es un programa de software que extrae datos de una aplicación de origen, como, por ejemplo, IBM Tivoli Monitoring o IBM Tivoli Business Service Manager.

Cada DLA escribe archivos XML que contienen información sobre recursos en un determinado formato XML denominado IdML (Identity Markup Language). Se hace referencia a cualquier archivo XML escrito en el formato IdML como *libro*. Para ver la colección de libros de Tivoli que puede cargar la base de datos de TADDM con los datos de otros productos de Tivoli, consulte http://www.ibm.com/software/brandcatalog/ismlibrary/.

Los DLA son específicos de un determinado producto, puesto que cada producto tiene un método distinto para acceder a los recursos del entorno. La configuración y la instalación de un DLA es diferente para cada aplicación. Un DLA típico está instalado en un sistema que tiene acceso a datos de una aplicación determinada. Por ejemplo, el DLA de IBM Tivoli Monitoring está instalado en un sistema que tiene acceso a la base de datos del sistema de gestión empresarial de IBM Tivoli Monitoring. Todos los DLA se ejecutan utilizando la interfaz de línea de mandatos y se pueden planificar para que se ejecuten utilizando cualquier tipo de programa de planificación (por ejemplo, cron).

Un DLA se puede crear para extraer información de productos o bases de datos existentes en el entorno.

Para obtener más información acerca de cómo crear un DLA y acerca de la especificación IdML o para obtener detalles adicionales sobre el almacén de biblioteca de descubrimiento, consulte *Discovery Library Adapter Developer's Guide* (Guía del desarrollador del adaptador de biblioteca de descubrimiento) de TADDM.

Acerca de esta tarea

Normalmente, el almacén de biblioteca de descubrimiento está ubicado en el servidor de TADDM. Si no configura el almacén de biblioteca de descubrimiento en el servidor de TADDM, debe asegurarse de que el programa de carga masiva de TADDM que se ejecute en el servidor de TADDM pueda acceder al almacén de biblioteca de descubrimiento. Se pueden ejecutar otras aplicaciones en el mismo sistema que aloja el almacén de biblioteca de descubrimiento.

Procedimiento

Para crear el almacén de biblioteca de almacenamiento, efectúe los pasos siguientes:

1. Cree un directorio para almacenar los archivos XML en un sistema, con un nombre de directorio que se distinga (por ejemplo, `c:\IBM\DLFS`). De forma opcional, puede crear subdirectorios en el almacén de biblioteca de descubrimiento principal para cada DLA que tenga la intención de utilizar.
2. Configure un protocolo de transferencia de archivos (FTP) con al menos un ID de usuario. El ID de usuario debe disponer de los siguientes permisos: acceso de escritura, reasignación de nombres y lectura para el directorio en el que se almacenan los archivos XML de la biblioteca de descubrimiento. Si no utiliza FTP para trasferir los archivos XML al almacén de biblioteca de descubrimiento, asegúrese de que la herramienta que elija, y el ID de usuario empleado para ejecutar la misma, tengan permisos de escritura en el directorio del almacén de biblioteca de descubrimiento.
3. Asegúrese de que los diversos adaptadores de biblioteca de descubrimiento tengan acceso al nombre del sistema (nombre de host) en el que se aloje el almacén de biblioteca de descubrimiento. La mayoría de los adaptadores de biblioteca de descubrimiento copiarán archivos XML en el almacén de biblioteca de descubrimiento.
4. Asegúrese de que los diversos adaptadores de biblioteca de almacenamiento tengan el ID de usuario y la contraseña necesarios para conectarse al servidor FTP.
5. Si el DLA no utiliza FTP, copie los archivos XML (libros) a los que desea que el programa de cargador masivo acceda en este directorio compartido. El programa de cargador masivo debe poder acceder al directorio compartido.

   Es responsabilidad de los escritores de libros y del administrador colocar los libros en el almacén de biblioteca de descubrimiento. Un ejemplo es configurar un trabajo cron para enviar los libros IdML producidos al almacén del adaptador de biblioteca de descubrimiento mediante FTP.

Qué hacer a continuación

Si va a crear un almacén de biblioteca de descubrimiento y desea configurar una base de datos de TADDM para que contenga libros del DLA, una unidad local en el servidor del dominio puede ser el almacén de biblioteca de descubrimiento en red. Este directorio se puede definir en el archivo `$COLLATION_HOME/etc/bulkload.properties` del servidor del dominio en el que se cargan los datos. Si dispone de varios servidores de dominio, configure el programa de cargador masivo correcto para acceder al directorio compartido correspondiente. El cargador masivo no suprime archivos XML del almacén de biblioteca de descubrimiento. Debe conservar los archivos en el almacén de biblioteca de descubrimiento. Asegúrese de que haya suficiente espacio en disco en el servidor para poder alojar los archivos en el directorio. Si se añaden con frecuencia nuevos archivos XML al directorio, debería limpiar éste de forma regular.

Si dispone de un despliegue de servidor de sincronización, debe elegir entre las opciones siguientes:

- Si los recursos a los que se hace referencia en un libro están contenidos en las definiciones de ámbito que se han definido en un único servidor de dominio, cargue ese libro en el servidor de dominio respectivo.

- Si los recursos a los que se hace referencia en un libro ***no*** están contenidos en las definiciones de ámbito que se han definido en un único servidor de dominio, cargue todos los libros en el servidor de sincronización.

Configuración para iniciar en contexto

Para ver información más detallada sobre los componentes de su entorno, puede iniciar las vistas de TADDM desde otras aplicaciones de Tivoli. Para configurar su aplicación para que inicie vistas de TADDM en contexto, debe especificar un URL.

Vistas que puede iniciar desde otras aplicaciones de Tivoli

Desde otras aplicaciones Tivoli, puede iniciar vistas del Portal de gestión de datos. También puede iniciar el informe de detalles y de historial de cambios para un elemento de configuración (CI) que se haya especificado.

En las vistas del Portal de gestión de datos, puede ver más información para las siguientes agrupaciones de componentes:

- Aplicaciones empresariales
- Servicios empresariales
- Colecciones

Si tanto el servidor de TADDM como la aplicación desde la que se inicia éste no se han configurado para un inicio de sesión único, aparece una ventana de inicio de sesión. Para poder ver información adicional en el Portal de gestión de datos, debe proporcionar un nombre de usuario y una contraseña.

Especificación del URL para iniciar vistas de TADDM

Para iniciar vistas de TADDM en contexto desde otras aplicaciones de Tivoli, debe especificar una URL.

El formato URL para iniciar en contexto:

Protocolo://*nombre_host_TADDM*:*puerto_TADDM*/*Raíz_contexto*/?*Serie_consulta*

En la lista siguiente se describen los valores válidos para cada variable en el formato URL:

Protocolo
Protocolo web que hay que utilizar. Los valores válidos son `http` o `https`.

nombre_host_TADDM
El nombre de host del servidor de TADDM respecto al cual efectúa la acción de inicio.

puerto_TADDM
El número de puerto del servidor de TADDM respecto al cual efectúa la acción de inicio. El valor predeterminado es `9430`.

Raíz_contexto
Los valores siguientes son válidos:

cdm/servlet/LICServlet
La vía de acceso relativa al servlet Java desplegado en el servidor Apache Tomcat para TADDM 7.3.0 y en el servidor de perfil WAS Liberty para TADDM 7.3.0.1 y posterior.

cdm/queryHomePage.do
La vía de acceso relativa a la página inicial de consultas, cuando se lanzó desde IBM Tivoli Monitoring, mediante inicio de sesión único y especificando el texto de búsqueda.

Serie_consulta

Contiene parámetros de par nombre-valor que están delimitados por separadores. El formato para un par nombre -valor es `name=value`. Utilice el carácter `=` para separar nombres y valores, y utilice el carácter `&` para separar pares nombre-valor.

En la lista siguiente se describen los pares nombre-valor válidos que pueden utilizarse en la variable *Serie_consulta*:

`view`

Especifica que desea visualizar el historial de cambios.

El único valor válido es `changehistory`.

`days_previous`

Especifica el período de tiempo (el número de días que han pasado) para el cual se debe mostrar el historial de cambios de un elemento de configuración en particular.

El valor válido es un entero positivo.

`hoursback`

Especifica el periodo de tiempo (número de horas que han pasado) para el cual se debe mostrar el historial de cambios de un elemento de configuración concreto.

El valor válido es un entero positivo.

`Guid`

Especifica el identificador exclusivo global (GUID) de un elemento de configuración.

Para el servidor de dominio y el servidor de sincronización, Tabla 47 en la página 227 lista los valores válidos para el parámetro `graph` e indica si el parámetro `guid` es opcional o necesario según el valor del gráfico respectivo.

Si se especifica el parámetro `graph` con cualquiera de los valores siguientes, el parámetro `guid` es opcional:

- `businessapplications`
- `applicationinfrastructure`
- `physicalinfrastructure`

Si se especifica el parámetro `graph` con cualquier otro tipo de gráfico de topología, se necesita el parámetro `guid`.

El valor válido es una representación de serie válida de un GUID, tal como se muestra en el ejemplo siguiente:

```
BA2842345F693855A3165A4B5F0D8BDE
```

Debe especificar sólo un GUID para cada solicitud de URL para el inicio en contexto.

`graph`

Especifica el tipo de gráfico de topología que se va a iniciar.

Si también especifica un elemento de configuración proporcionando su GUID en el parámetro `guid`, entonces se selecciona el elemento de configuración solicitado, si se encuentra en el gráfico de topología que se haya especificado en este parámetro `graph`.

Para el servidor de dominio y el servidor de sincronización, Tabla 47 lista los valores válidos para el parámetro `graph` e indica si el parámetro `guid` es opcional o necesario según el valor del gráfico respectivo.

Tabla 47. Valores de gráfico válidos y las relaciones correspondientes al parámetros `guid`

	Valor válido	**¿Es opcional o necesario el parámetro `guid` con este valor de gráfico?**
Servicio del dominio	`businessapplications`	Opcional
	`applicationinfrastructure`	Opcional
	`physicalinfrastructure`	Opcional
	Para los objetos de colección personalizada: • `ba_infrastructure`	Necesario
Servidor de sincronización	`businessapplications`	Opcional
	`physicalinfrastructure`	Opcional
	Para los objetos de colección personalizada: • `ba_infrastructure`	Necesario

Nota: Los otros tipos de gráficos que se utilizaban en los releases de TADDM anteriores para representar determinadas entidades de agrupación por GUID están en desuso. No obstante, para garantizar la compatibilidad con versiones anteriores, si especifica un tipo de gráfico antiguo con un GUID, la solicitud se redirecciona al nuevo tipo de topología.

`username`
Especifica el nombre de usuario utilizado para iniciar la sesión en TADDM.

`password`
Especifica la contraseña utilizada para iniciar la sesión en TADDM.

`launchsource`
El único valor válido es `ITM`. Siempre se utiliza con el par nombre-valor de `searchtext=`*`search_term`*.

La búsqueda está limitada a los elementos de configuración de tipo ComputerSystem y TMSAgent, listados en el archivo de configuración`$COLLATION_HOME/etc/cdm/xml/itm_query_components.xml`.

Desde los resultados de la página de inicio de consulta, para cada elemento de configuración listado, puede lanzar las siguientes vistas:

- Panel de historial de cambios
- Panel de detalles
- Portal de gestión de datos, visualización del panel Detalles

`searchtext`
Especifica el término de búsqueda. Siempre se utiliza con el par nombre-valor`launchsource=ITM`.

Ejemplos de cómo especificar el URL

En los ejemplos siguientes se muestra cómo especificar el URL para iniciar vistas de TADDM:

URL para lanzar el portal de gestión de datos, sin especificar información de autorización de forma separada.

```
http://home.taddm.com:9430/cdm/servlet/LICServlet?username=administrator
&password=adminpwd&guid=BA2842345F693855A3165A4B5F0D8BDE
```

Si utiliza una conexión acreditada, debe utilizar sólo credenciales como parte del URL para el inicio en contexto porque el usuario y la contraseña no están cifrados.

El URL para iniciar la ventana Página inicial de consulta para IBM Tivoli Monitoring cuando se utiliza el inicio de sesión único y la búsqueda de un elemento de configuración que coincida con el texto de búsqueda

```
http://home.taddm.com:9430/cdm/queryHomePage.do?launchsource=itm&searchtext=127.0.0.1
```

URL para mostrar una topología de una colección personalizada indicada por el parámetro `guid`

```
http://home.taddm.com:9430/cdm/servlet/LICServlet?username=administrator
&password=adminpwd&graph=ba_infrastructure&guid=BA2842345F693855A3165A4B5F0D8BDE
```

Envío de sucesos de cambio a sistemas externos

Puede configurar TADDM para que notifique a un sistema externo de manejo de sucesos que se ha detectado un cambio en un recurso descubierto.

Para enviar sucesos de cambio desde TADDM, debe tener instalados uno o más de los sistemas de manejo de sucesos siguientes:

- IBM Tivoli Monitoring 6.2.1 fixpack 2, o posterior
- IBM TivoliNetcool/OMNIbus, incluido el analizador Event Integration Facility (EIF)

Para ver las versiones soportadas de los productos, vaya a la sección "Versiones soportadas" en la página 200.

Al finalizar un descubrimiento, TADDM verifica si se han producido cambios en aquellos elementos de los cuales los sistemas externos de manejo de sucesos realizan un seguimiento. Si no se detecta ninguno, se envían los elementos, mediante EIF, directamente a IBM Tivoli Netcool/OMNIbus y a IBM Tivoli Monitoring mediante el agente universal.

El Agente universal convierte las notificaciones recibidas en sucesos asíncronos, y reenvía los datos al componente IBM Tivoli Enterprise Monitoring Server de IBM Tivoli Monitoring. IBM Tivoli Monitoring Server almacena los sucesos y los utiliza para evaluar las situaciones. Entonces, los sucesos se pasan a IBM Tivoli Enterprise Portal para su visualización.

Los servidores de IBM Tivoli Netcool/OMNIbus procesan los sucesos recibidos según las reglas internas y los muestran.

Para configurar el envío de los sucesos de cambio desde TADDM a los sistemas externos de manejo de sucesos, debe habilitar los sucesos de cambio en TADDM, y configurar cada destinatario externo para que maneje los sucesos entrantes, según convenga.

Configuración de TADDM para enviar eventos de cambio

Para enviar sucesos de cambio, debe configurar TADDM con información sobre los sistemas de manejo de sucesos a los que desee enviar los sucesos de cambio.

Acerca de esta tarea

Según el tipo de despliegue de TADDM, realice los siguientes cambios en los servidores de TADDM:

- En un despliegue de servidor de dominio, realice los cambios en el servidor del dominio.
- En un despliegue de servidor de sincronización, realice los cambios en el servidor de sincronización.
- En un despliegue de servidor de modalidad continua, realice los cambios en el servidor de almacenamiento primario.

Procedimiento

Para habilitar el envío de información de sucesos de cambio, realice los pasos siguientes:

1. Para habilitar los sucesos de cambio establezca, en el archivo `$COLLATION_HOME/etc/collation.properties`, la propiedad siguiente: `com.ibm.cdb.omp.changeevent.enabled=true`.
2. Para configurar a qué recursos se les realiza un seguimiento en busca de cambios, y a qué sistemas de manejo de sucesos se envían los sucesos, edite el archivo `$COLLATION_HOME/etc/EventConfig.xml`.

   Para obtener información sobre el formato que debe utilizar para especificar información en el archivo`EventConfig.xml`, consulte "Configuración del módulo de sucesos de cambio de OMP de TADDM".

   Cuando se actualiza TADDM, el archivo `EventConfig.xml` de la versión anterior de TADDM se conserva para asegurar que no se pierdan los ajustes personalizados que había configurado. Hay información disponible sobre las nuevas funciones y cómo utilizarlas en el archivo de `$COLLATION_HOME/etc/EventConfigDefault.xml`. El archivo de `EventConfigDefault.xml` es sólo para referencia. Si desea utilizar alguna de las nuevas funciones, debe actualizar `EventConfig.xml` basándose en los ejemplos apropiados de `EventConfigDefault.xml`.
3. Si había especificado un sistema de manejo de sucesos IBMTivoliNetcool/OMNIbus en el archivo `EventConfig.xml`, cree el correspondiente archivo de propiedades EIF para cada tipo de sistema. Para ello, realice los pasos siguientes:
   a. Cree un archivo de propiedades `$COLLATION_HOME/etc/omnibus.eif.properties`.
   b. Personalice el archivo `omnibus.eif.properties`. Para obtener más información acerca de cómo personalizar un archivo de propiedades EIF, consulte *Configuración del soporte de sucesos de TADDM en el entorno integrado* en http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_7.4.0/com.ibm.netcool_OMNIbus.doc_7.4.0/omnibus/wip/install/task/omn_con_ext_configuringtaddmevents.html?lang=en en la documentación de IBM Tivoli Netcool/OMNIbus.

Configuración del módulo de sucesos de cambio de OMP de TADDM:

Para habilitar el envío de sucesos de cambio, debe editar el archivo `EventConfig.xml` para definir escuchas y destinatarios de sucesos.

Escuchas de sucesos

Puede definir un escucha proporcionando los criterios necesarios para una consulta de TADDM. Los objetos resultantes que selecciona la consulta se comprueba si cambian después de cada descubrimiento. Puede haber varios escuchas. Debe existir un bloqueo de escucha y destinatario correspondiente para que se produzca un suceso de direccionamiento.

Utilice el siguiente formato para especificar un escucha.

```
<listener object="[OBJECT_TYPE]"
          enabled="true|false">
          sendCauses="true|false"
          sendOriginGuid="true|false">
   <alert recipient="[RECIPIENT_SYSTEM_NAME]"/>
   <attribute name="[ATTRIBUTE_NAME]" operator="[OPERATOR]">
     <value>
     [ATTRIBUTE_VALUE]
     </value>
   </attribute>
   <causeFilter object="[CAUSEFILTER_OBJECT_TYPE]"
                sendOriginGuid="true|false"/>

 </listener>
```

donde:

[OBJECT_TYPE]
es un tipo de objeto de modelo que se representa en TADDM, por ejemplo, ComputerSystem o ITSystem. Para ver más ejemplos, consulte el diccionario de datos de TADDM en `http://host_servidor_taddm:9430/cdm/datadictionary/model-object/index.html`.

enabled
es un atributo que permite el envío de los sucesos. El valor debe establecerse en `true` para que el escucha esté activo.

sendCauses
es un atributo opcional que define si el escucha envía sucesos sobre los cambios que se han propagado en el objeto de modelo. Por ejemplo, si un cambio en un sistema operativo Windows provoca un cambio en un objeto ComputerSystem y el atributo `sendCauses` está establecido en `true` para un escucha de ComputerSystem, el escucha envía un suceso del cambio a ComputerSystem y al sistema operativo Windows. El valor predeterminado del atributo `sendCauses` es `false`.

sendOriginGuid
es un atributo opcional que se utiliza con el atributo `sendCauses`. Cuando el atributo `sendOriginGuid` se establece en `true`, un objeto que coincida con el escucha se considera el origen lógico de los cambios que se propagan al objeto. Los sucesos que se envían sobre los cambios propagados contienen el identificador exclusivo del objeto de origen. Por ejemplo, si un cambio en un objeto ConfigFile genera un cambio en un objeto ComputerSystem y los atributos `sendCauses` y `sendOriginGuid` están establecidos en `true` para un escucha de ComputerSystem, el suceso sobre el cambio de ConfigFile contiene el identificador exclusivo del objeto ComputerSystem, además el identificador exclusivo del objeto ConfigFile. Esta función sólo está disponible para los destinatarios de sucesos de Netcool/OMNIbus. El valor predeterminado del atributo `sendOriginGuid` es false.

[RECIPIENT_SYSTEM_NAME]
es un destinatario de alerta. Consulte “Destinatarios de sucesos” en la página 232.

[ATTRIBUTE_NAME]
es el nombre de un atributo en `[OBJECT_TYPE]` que se consulta.

[OPERATOR]
es el nombre del operador de una consulta MQL de TADDM. Se permiten los siguientes valores.

Tabla 48. Nombres de operador de una consulta MQL de TADDM..

Operador	Equivalente de MQL de TADDM
contains-with	contains
ends-with	ends-with
equals	equals
greater-or-equal	>=
greater-than	>
less-or-equal	<=
less-than	<
not-equals	not-equals
starts-with	starts-with

[ATTRIBUTE_VALUE]
es el valor con el que se evalúa el atributo.

<causeFilter>
es un atributo que proporciona un medio de filtrar los tipos de objeto de los sucesos de causa que se pasan cuando el atributo `sendCauses` está habilitado. Si especifica este atributo, solo se envían los sucesos de causa del tipo de objeto especificado. No obstante, los sucesos propagados continúan enviándose, por ejemplo, los que forman parte del tipo de objeto que se ha especificado en el escucha. Si el atributo `causeFilter` no se especifica, todos los sucesos de causa que encuentre el escucha se enviarán al destinatario.

Por ejemplo, un cambio en WindowsService genera un cambio en el sistema operativo Windows y, por lo tanto, en ComputerSystem. Si establece el atributo `causeFilter` en WindowsService, sólo se muestran los cambios de ComputerSystem y WindowsService; el cambio en el sistema operativo Windows no se muestra.

Cuando establece el atributo `causeFilter`, también puede establecer un valor para el atributo `sendOriginGuid`. De forma predeterminada, el atributo `causeFilter` hereda el valor `sendOriginGuid` del escucha que es el padre del atributo `causeFilter`. Cuando utiliza el atributo `sendOriginGuid` en un atributo `causeFilter`, sólo se altera temporalmente el valor de escucha de ese atributo `causeFilter`.

Si desea actualizar objetos como WindowsService o ConfigFile, cuyos cambios se propagan a un objeto de nivel superior como ComputerSystem, capture estos objetos utilizando una combinación de los atributos `sendCauses` y `causeFilter`, en lugar de un escucha aparte.

[CAUSEFILTER_OBJECT_TYPE]
es el nombre de clase del objeto definido en el CDM. Puede utilizar el

nombre completo, por ejemplo, `com.collation.platform.model.topology.sys.windows.WindowsService`, o el nombre abreviado, por ejemplo, `WindowsService`.

Ejemplos de escuchas de sucesos

En el siguiente ejemplo, un cambio que se ha detectado en cualquier ComputerSystem cuyo FQDN contiene la serie `"mycompany"` se envía al destinatario `"enterprise-eventhost-itm"`.

```
<listener object="ComputerSystem" enabled="true">
  <alert recipient="enterprise-eventhost-itm"/>
  <attribute name="fqdn" operator="contains-with">
    <value>
     mycompany
    </value>
  </attribute>
</listener>
```

En el siguiente ejemplo, se detectan los cambios en todos los objetos de un tipo especificado.

```
  <attribute name="guid" operator="not-equals">
    <value>
     0
    </value>
  </attribute>
```

En el siguiente ejemplo, un cambio que se ha detectado en un objeto del tipo ComputerSystem se envía al destinatario `"enterprise-eventhost-omnibus"`.

```
<listener object="ComputerSystem" enabled="true">
  <alert recipient="enterprise-eventhost-omnibus"/>
  <attribute name="guid" operator="not-equals">
    <value>
     0
    </value>
  </attribute>
</listener>
```

En el ejemplo siguiente, sólo se envían los cambios debidos a un cambio en un ConfigFile en un sistema Linux.

```
<listener object="ITSystem" enabled="true" sendCauses="true">
  <alert recipient="enterprise-eventhost-itm"/>
  <attribute name="name" operator="ends-with">
  <value>
    ShoppingCart
  </value>
  </attribute>
  <causeFilter object="ConfigFile" />
  <causeFilter object="LinuxUnitaryComputerSystem" />
</listener>
```

Destinatarios de sucesos

Un destinatario de sucesos es una instancia de IBM Tivoli Monitoring u OMNIBus que puede recibir sucesos del módulo de sucesos de cambio. Cuando los escuchas de cambios ubican los cambios, se envía una notificación a los destinatarios correspondientes. Puede definir varios destinatarios de tipo diferente o del mismo tipo de forma simultánea. Debe existir un bloqueo de escucha y destinatario correspondiente para que se produzca un suceso de direccionamiento.

Utilice el siguiente formato para especificar un destinatario.

```
<recipient name="[RECIPIENT_NAME]" type="[RECIPIENT_TYPE]">
  <address>[RECIPIENT_FQDN]</address>
  <port>[EVENT_ROUTING_PORT]</port>
  <config>[PATH_TO_EIF_CONFIGURATION]</config>
</recipient>
```

donde:

[RECIPIENT_NAME]
es el nombre del sistema que aparece en el escucha.

[RECIPIENT_TYPE]
es el tipo de software que se utiliza para recibir los sucesos. Los tipos siguientes están soportados:

- `itm`: IBM Tivoli Monitoring 6 con el proveedor de datos POST del Agente universal.
- `omnibus`: Netcool/OMNIbus con el adaptador EIF.

[RECIPIENT_FQDN]
(Sólo para IBM Tivoli Monitoring) es el nombre de dominio completo del host donde se encuentra el Agente universal.

[EVENT_ROUTING_PORT]
(Sólo para IBM Tivoli Monitoring) es el puerto que ha especificado el proveedor de datos POST del Agente universal en `KUMENV` como `KUMP_POST_DP_PORT`.

[PATH_TO_EIF_CONFIGURATION]
(Sólo para OMNIBUS) es la vía de acceso de la configuración de EIF, que se lee en el archivo de propiedades. Utilice la vía de acceso completa del archivo.

Ejemplos de destinatarios de sucesos

El siguiente ejemplo define un destinatario de sucesos de Netcool/OMNIbus.

```
<recipient name="enterprise-eventhost-omnibus" type="omnibus">
  <config>/opt/IBM/taddm/dist/etc/omnibus.eif.properties</config>
</recipient>
```

El siguiente ejemplo define un destinatario de sucesos de IBM Tivoli Monitoring.

```
<recipient name="enterprise-eventhost-itm" type="itm">
  <address>itm-ua.mycompany.com</address>
  <port>7575</port>
</recipient>
```

Configuración de IBMTivoliNetcool/OMNIbus

Puede configurar IBMTivoliNetcool/OMNIbus Versión 7.3 o posterior para recibir sucesos de cambio enviados por TADDM. Puede agregar y personalizar los datos de suceso que se visualizan en las versiones anteriores de Tivoli Netcool/OMNIbus y puede definir la lógica de manejo de sucesos.

Antes de empezar

Para configurar IBM Tivoli Netcool/OMNIbus Versión 7.3 o posterior para recibir sucesos de cambio que envía TADDM, consulte el tema *Enabling support for TADDM events* en la documentación de IBM Tivoli Netcool/OMNIbus en http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html?lang=en. La documentación de Tivoli Netcool/OMNIbus también incluye información acerca del archivo `tivoli_eif_taddm.rules`. Este

archivo contiene la lógica para procesar detalles acerca de los cambios de configuración que se han detectados durante un descubrimiento de TADDM.

En un entorno en el que se utiliza cálculo de alta disponibilidad o la migración tras error, TADDM se puede configurar para dar soporte a la migración tras error automática. Este soporte se lleva a cabo cuando los sucesos TADDM se envían a Tivoli Netcool/OMNIbus. Puede especificar las direcciones primaria y secundaria del analizador EIF y sus puertos asociados en el archivo de propiedades EIF. El ejemplo siguiente muestra dónde se han de añadir estas propiedades:

```
#
Nombre de host donde reside el analizador EIF de NetCool/OMNIbus.  Especifique
hasta 8 ubicaciones.
# Cada ubicación se debe separa con una coma.
# El suceso se envía al primer analizador disponible de la lista.
# Ejemplo:
#     ServerLocation=netcool.mycompany.com,netcool2.mycompany.com
ServerLocation=netcool.mycompany.com,netcool2.mycompany.com

# Puerto donde escucha el analizador EIF de NetCool/OMNIbus.
# Debe haber una entrada de puerto para cada analizador en ServerLocation.
# Ejemplo:
#     ServerPort=9998,9998
ServerPort=9998,9998
```

Cada dirección de analizador debe tener especificado el puerto asociado en la propiedad *ServerPort*. Si no se especifica el puerto de cada dirección de analizador, se genera un error cuando se envía el suceso. Cuando no se puede enviar un suceso al puerto primario, se envía al primer puerto disponible de la lista. Se pueden especificar hasta ocho direcciones de puerto en la propiedad *ServerLocation*.

Acerca de esta tarea

En las versiones de IBMTivoliNetcool/OMNIbus anteriores a la versión 7.3, el comportamiento predeterminado es para todos los sucesos desde un módulo de sucesos que se ha de combinar en un solo sucesos, con el atributo de recuento establecido de modo que visualice el número de sucesos contenidos en el suceso combinado. En los siguientes pasos se describe cómo cambiar el comportamiento predeterminado.

Procedimiento

1. En el servidor de TADDM, abra el archivo siguiente, para editarlo: `$COLLATION_HOME/etc/omnibus.eif.properties`
2. Establezca los valores de propiedad de las propiedades TADDMEvent_Slot siguientes:

```
TADDMEvent_Slot_object_name=$TADDM_OBJECT_NAME
TADDMEvent_Slot_change_type=$TADDM_CHANGE_TYPE
TADDMEvent_Slot_change_time=$TADDM_CHANGE_TIME
TADDMEvent_Slot_class_name=$TADDM_CLASS_NAME
TADDMEvent_Slot_attribute_name=$TADDM_ATTRIBUTE_NAME
TADDMEvent_Slot_old_value=$TADDM_OLD_VALUE
TADDMEvent_Slot_new_value=$TADDM_NEW_VALUE
TADDMEvent_Slot_host=$TADDM_HOST
TADDMEvent_Slot_port=$TADDM_PORT
TADDMEvent_Slot_guid=$TADDM_GUID
TADDMEvent_Slot_origin=$TADDM_ORIGIN
```

Qué hacer a continuación

Si experimenta problemas al configurar IBM Tivoli Netcool/OMNIbus, consulte el tema *Problemas de integración de TADDM con otros productos* de la *Guía de resolución de problemas* de TADDM.

Configuración de un proveedor de datos de IBM Tivoli Monitoring

Puede configurar el archivo de inicialización del Agente universal para que defina un proveedor de datos nuevo.

Antes de empezar

Si utiliza Tivoli Monitoring versión 6.2.2 o anterior, asegúrese de que no hay tabuladores ni caracteres de espacio en el archivo de configuración `KUMPOST`.

Procedimiento

Para configurar un proveedor de datos de IBM Tivoli Monitoring, realice los pasos siguientes:

Si ejecuta el agente universal en un sistema Windows, realice los pasos siguientes:

1. En el sistema Windows donde está instalado el agente universal, pulse **Iniciar** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
2. Pulse el botón derecho del ratón en el Agente universal y pulse **Reconfigurar**.
3. En cada una de las dos ventanas Configuración avanzada de agente, pulse **Aceptar**.
4. Para actualizar el archivo de inicialización del Agente universal, pulse **Sí**. Se abre el archivo KUMENV en el editor de texto del sistema.
5. Establezca el valor KUMA_STARTUP_DP en `POST`:

   ```
   KUMA_STARTUP_DP=POST
   ```

   Nota: Si el agente universal ya está configurado para que utilice otro proveedor de datos, especifique ambos valores separados por comas, como en el siguiente ejemplo:

   ```
   KUMA_STARTUP_DP=ASFS,POST
   ```

6. Añada la información necesaria del parámetro POST al archivo KUMENV:

   ```
   *---------------------------------------*
   * Parámetros de DP (proveedor de datos) POST de TADDM *
   *---------------------------------------*
   KUMP_POST_DP_PORT=7575
   KUMP_POST_GROUP_NAME=TADDM
   KUMP_POST_APPL_TTL=14400
   ```

7. Guarde el archivo KUMENV, y ciérrelo.
8. Para configurar el agente, pulse **Sí**.
9. En la ventana Gestionar servicios de Tivoli Enterprise Monitoring, pulse el botón derecho del ratón en **Agente universal** > **Inicio**.
10. En el editor de texto del sistema, cree un archivo de texto. Escriba la información siguiente en el archivo:

    ```
    //APPl CONFIGCHANGE
    //NAME dpPost E 3600
    //ATTRIBUTES ';'
    Post_Time T 16 Caption{Time}
    Post_Origin D 32 Caption{Origination}
    Post_Ack_Stamp D 28 Caption{Event time stamp}
    ```

```
Comp_Type D 512 Caption{Component type}
Comp_Name D 512 Caption{Component name}
Comp_Guid D 512 Caption{Component GUID}
Change_Type D 512 Caption{Change type}
Chg_Det_Time D 512 Caption{Change detection time}
Chg_Attr D 512 Caption{Changed attribute}
Srv_Addr D 512 Caption{TADDM server}
Srv_Port D 16 Caption{TADDM port}
```

11. Guarde el archivo como %ITM_HOME%\TMAITM6\metafiles\KUMPOST.

    Nota: Asegúrese de haber escrito bien el nombre del archivo, KUMPOST, en mayúsculas, tal como aparece aquí.
12. Abra un indicador de mandatos de Windows, y vaya hasta la carpeta %ITM_HOME%\TMAITM6.
13. Ejecute el programa KUMPCON.exe para validar e importar el metarchivo KUMPOST.
14. En la ventana Gestionar servicios de Tivoli Monitoring, pulse el botón derecho del ratón en el Agente universal y seleccione **Reiniciar**.

Si ejecuta el agente universal en un sistema Linux o UNIX, realice los pasos siguientes:

1. Reconfigure el Agente universal, mediante el mandato siguiente:

   ```
   itmcmd config – A um
   ```

   Cuando se le solicite el nombre del proveedor de datos, escriba POST.

   Nota: Si el agente universal ya está configurado para utilizar otro proveedor de datos, especifique los dos valores separados por comas (por ejemplo, ASFS,POST).
2. En el directorio $ITM_HOME/config, efectúe una copia de seguridad del archivo um.ini y, a continuación, añada las entradas siguientes a la copia original del archivo:

   ```
   # Parámetros de DP (proveedor de datos) POST de TADDM
   KUMP_POST_DP_PORT=7575
   KUMP_POST_GROUP_NAME=TADDM
   KUMP_POST_APPL_TTL=14400
   ```
3. En el directorio $ITM_HOME/*interp*/um/metafiles, cree un archivo de texto. Escriba la información siguiente en el archivo:

   ```
   //APPl CONFIGCHANGE
   //NAME dpPost E 3600
   //ATTRIBUTES ';'
   Post_Time T 16 Caption{Time}
   Post_Origin D 32 Caption{Origination}
   Post_Ack_Stamp D 28 Caption{Event time stamp}
   Comp_Type D 512 Caption{Component type}
   Comp_Name D 512 Caption{Component name}
   Comp_Guid D 512 Caption{Component GUID}
   Change_Type D 512 Caption{Change type}
   Chg_Det_Time D 512 Caption{Change detection time}
   Chg_Attr D 512 Caption{Changed attribute}
   Srv_Addr D 512 Caption{TADDM server}
   Srv_Port D 16 Caption{TADDM port}
   ```
4. Guarde el archivo como KUMPOST.

   Nota: Asegúrese de haber escrito bien el nombre del archivo, KUMPOST, en mayúsculas, tal como aparece aquí.
5. Reinicie el Agente universal, mediante los mandatos siguientes:

```
itmcmd agent stop um
itmcmd agent start um
```

6. Para validar y renovar el metarchivo KUMPOST, efectúe los siguientes pasos:
   a. Ejecute el mandato $ITM_HOME/bin/um_console con los siguientes parámetros:
      ```
      um_console -h <directorio de ITM>
      ```
   b. En la línea de mandatos, escriba el siguiente texto:
      ```
      validate KUMPOST
      ```
      Se mostrarán una serie de mensajes parecidos a estos:
      ```
      KUMPS001I Entrada de consola aceptada.
      KUMPV025I Procesando metarchivo de entrada /opt/IBM/ITM//lx8266/um/metafiles/KUMPOST
      KUMPV026I Procesando registro 0001 -> //APPl CONFIGCHANGE
      KUMPV148I Nota: los nombres APPL que empiezan por las letras A-M están designados para
      las soluciones Best Practices y Business Partner UA.
      KUMPV026I Procesando registro 0002 ->     //NAME dpPost E 3600
      KUMPV026I Procesando registro 0003 ->     //ATTRIBUTES ';'
      KUMPV026I Procesando registro 0004 -> Post_Time T 16 Caption{Time}
      KUMPV026I Procesando registro 0005 -> Post_Origin D 32 Caption{Origination}
      KUMPV026I Procesando registro 0006 -> Post_Ack_Stamp D 28 Caption{Event time stamp}
      KUMPV026I Procesando registro 0007 -> Comp_Type D 512 Caption{Component type}
      KUMPV026I Procesando registro 0008 -> Comp_Name D 512 Caption{Component name}
      KUMPV026I Procesando registro 0009 -> Comp_Guid D 512 Caption{Component GUID}
      KUMPV026I Procesando registro 0010 -> Change_Type D 512 Caption{Change type}
      KUMPV026I Procesando registro 0011 -> Chg_Det_Time D 512 Caption{Change detection time}
      KUMPV026I Procesando registro 0012 -> Chg_Attr D 512 Caption{Changed attribute}
      KUMPV026I Procesando registro 0013 -> Srv_Addr D 512 Caption{TADDM server}
      KUMPV026I Procesando registro 0014 -> Srv_Port D 16 Caption{TADDM port}
      KUMPV000I La validación ha finalizado satisfactoriamente.
      KUMPV090I Se ha guardado el informe de validación de metarchivo de aplicación en un archivo.
      /opt/IBM/ITM//lx8266/um/metafiles/KUMPOST.rpt.
      ```
   c. Cuando se le solicite la acción que desea realizar en el metarchivo, escriba lo siguiente:
      ```
      Refresh
      ```
   d. Escriba Yes para confirmar.

Qué hacer a continuación

Para comprobar que la configuración del agente universal sea correcta, compruebe el informe de eventos de cambio en Tivoli Enterprise Portal.

Para abrir el informe de eventos de cambio utilizando IBM Tivoli Monitoring 6.2.1 o posterior, realice los pasos siguientes:

1. Navegue al agente universal configurado para enviar y recibir notificaciones de sucesos desde TADDM.
2. Expanda el nodo CONFIGCHANGE.
3. Pulse el nodo **DPPOST**.

Creación de situaciones de cambio de configuración en IBM Tivoli Monitoring

Puede utilizar la función Situación de Tivoli Enterprise Portal para supervisar los sucesos de cambio y desencadenar situaciones que dependen de la información que aparezca en un suceso de cambio.

Procedimiento

Para crear una situación de cambio de configuración en IBM Tivoli Monitoring, realice los pasos siguientes:

Para crear una situación de cambio de configuración si utiliza IBM Tivoli Monitoring 6.2.1, realice los pasos siguientes:

1. En el panel Navegador de IBM Tivoli Enterprise Portal, navegue hasta el agente universal que está configurado para enviar y recibir las notificaciones de sucesos de TADDM.
2. Expanda el nodo CONFIGCHANGE.
3. Pulse con el botón derecho el nodo DPPOST. Pulse **Situaciones**.
4. En la ventana "Situaciones de *nombre_nodo*", pulse con el botón derecho del ratón **Proveedor de datos universal**. Pulse **Crear nuevo**. Se visualiza la ventana Crear situación o regla.
5. En el campo **Nombre**, escriba el nombre de la situación. Por ejemplo, `ConfigurationChanged`.
6. En el campo **Descripción**, escriba una descripción de la situación. Por ejemplo, `TADDM ha detectado un cambio en un objeto del cual se realiza seguimiento`.
7. En la lista **Aplicación supervisada**, seleccione **Proveedor de datos universal**.
8. Asegúrese de que se haya deseleccionado el recuadro de selección **Correlacionar situaciones en sistemas gestionados**.
9. Pulse **Aceptar**. Se visualiza la ventana "Seleccionar condición".
10. En la lista **Grupo de atributos**, seleccione **DPPOST**.
11. En la lista **Elemento de atributo**, seleccione **Nombre de componente**.
12. Pulse **Aceptar**. Se visualiza el separador **Fórmula** correspondiente a la situación.
13. Configure la situación de forma que se desencadene cuando el nombre del componente coincida con el nombre del recurso del entorno que desee supervisar.
14. Pulse **Aceptar**.

Para crear una situación de cambio de configuración si utiliza IBM Tivoli Monitoring 6.2.2 o posterior, realice los pasos siguientes:

1. En el panel Navegador de IBM Tivoli Enterprise Portal, navegue hasta el agente universal que está configurado para enviar y recibir las notificaciones de sucesos de TADDM.
2. Expanda el nodo CONFIGCHANGE.
3. Pulse con el botón derecho el nodo DPPOST. Pulse **Situaciones**.
4. En la ventana "Situaciones de *nombre_nodo*", pulse **Crear situación nueva**. Se visualiza la ventana Crear situación.
5. En el campo **Nombre**, escriba el nombre de la situación. Por ejemplo, `ConfigurationChanged`.
6. En el campo **Descripción**, escriba una descripción de la situación. Por ejemplo, `TADDM ha detectado un cambio en un objeto del cual se realiza seguimiento`.
7. En la lista **Aplicación supervisada**, seleccione **Proveedor de datos universal**.
8. Pulse **Aceptar**. Se visualiza la ventana "Seleccionar condición".
9. En la lista **Grupo de atributos**, seleccione **DPPOST**.
10. En la lista **Elemento de atributo**, seleccione **Nombre de componente**.
11. Pulse **Aceptar**. Se visualiza el separador **Fórmula** correspondiente a la situación.

12. Configure la situación de forma que se desencadene cuando el nombre del componente coincida con el nombre del recurso del entorno que desee supervisar.
13. Pulse **Aceptar**.
14. En el panel Navegador de IBM Tivoli Enterprise Portal, pulse el botón derecho del ratón en el nodo que contenga el informe de suceso de cambio. Pulse **Situaciones**.
15. En la ventana "Situaciones de *nombre_nodo*", pulse con el botón derecho la situación **ConfiguraciónCambiada** que creó y pulse **Iniciar situación**.

Resultados

Cuando se reciban los sucesos de cambio de configuración, se comprobará su nombre de componente. Si el nombre de componente coincide con el del componente que haya especificado en la fórmula de la situación, se desencadena la situación configurada.

Creación de enlaces de detalles los informes de sucesos de cambios de la configuración en IBM Tivoli Monitoring

Puede crear enlaces dentro de una tabla de informe a un espacio de trabajo, donde se visualicen el historial de cambios y los detalles procedentes directamente del servidor de TADDM. Estos enlaces proporcionan información más detallada de la que aparece en un informe.

Procedimiento

Para crear un enlace, en un informe de sucesos de cambios de la configuración, a información de suceso de cambios más detallada, realice los pasos siguientes:

1. Para crear un espacio de trabajo en el que visualizar la información, realice los pasos siguientes:
   a. En el panel Navegador, pulse el botón derecho del ratón en el nodo en dentro del cual desee incluir el espacio de trabajo. Pulse **Archivo** > **Guardar espacio de trabajo como**. Se visualiza la ventana Guardar espacio de trabajo como.
   b. En el campo **Nombre**, escriba el nombre del espacio de trabajo. Por ejemplo, `ConfigChangeDetails`.
   c. En el campo **Descripción**, escriba una descripción del espacio de trabajo. Por ejemplo, `Espacio de trabajo genérico para la tabla se sucesos de cambio`.
   d. Seleccione el recuadro de selección **Sólo seleccionable como destino de un enlace de espacio de trabajo**.
   e. Pulse **Aceptar**.
2. Para configurar el espacio de trabajo utilizando IBM Tivoli Monitoring 6.2.1 o posterior, realice los pasos siguientes:
   a. Configure el espacio de trabajo para que tenga un panel Navegador a la izquierda y dos paneles de explorador a la derecha.
   b. Pulse **Editar** > **Propiedades**.
   c. En el panel Navegador, seleccione la primera instancia de **Cómo empezar**.
   d. En el panel Estilo, seleccione **Utilizar la ubicación proporcionada**.
   e. Pulse **Aceptar**.

f. En el campo **Ubicación** de uno de los paneles de navegador, escriba el URL de la vista Historial de cambios, en TADDM. Cuando haya escrito el URL en una línea, no pulse la tecla **Intro**.

```
http://$taddm_server$:$taddm_port$/cdm/servlet/
LICServlet?view=changehistory&hoursback=10000&console=web&guid=$taddm_guid$
```

El parámetro `hoursback` especifica el número de horas para el que se visualizan los sucesos de cambio. Por ejemplo, al establecer el parámetro `hoursback` en 6, se visualizan todos los sucesos de cambio de las seis horas anteriores.

g. En el panel Navegador, seleccione la segunda instancia de **Cómo empezar**.

h. En el panel Estilo, seleccione **Utilizar la ubicación proporcionada**.

i. Pulse **Aceptar**.

j. En el campo **Ubicación**, del segundo de los paneles de navegador, escriba el URL de la vista Detalles del objeto, en TADDM. Cuando haya escrito el URL en una línea, no pulse la tecla **Intro**.

```
http://$taddm_server$:$taddm_port$/cdm/servlet/LICServlet?console=web
&guid=$taddm_guid$
```

k. Para guardar el nuevo espacio de trabajo, pulse **Archivo** > **Guardar**.

Inmediatamente después que haber escrito el URL en el campo **Ubicación**, no pulse la tecla **Intro**, pero guarde el espacio de trabajo.

3. Abra IBM Tivoli Enterprise Portal. En el panel Informe, pulse el botón derecho del ratón en la tabla **Informe**.
4. Pulse **Enlazar a** > **Asistente de enlace**. Aparece la página de bienvenida del Asistente de enlace de espacio de trabajo.
5. Pulse **Crear un nuevo enlace**. Pulse **siguiente**. Aparece la página Nombre de enlace del Asistente de enlace de espacio de trabajo.
6. En el campo **Nombre**, escriba el nombre del enlace. Por ejemplo, `Mostrar los detalles`.
7. En el campo **Descripción**, escriba una descripción del enlace. Por ejemplo, `Enlazar a detalles`.
8. Pulse **siguiente**. Aparece la página Tipo de enlace del Asistente de enlace de espacio de trabajo.
9. Pulse **Absoluto**. Pulse **siguiente**. Aparece la página Espacio de trabajo de destino del Asistente de enlace de espacio de trabajo.
10. En el panel Navegador, seleccione el nodo que contenga el espacio de trabajo que haya creado. En el panel Espacio de trabajo, seleccione el espacio de trabajo que haya creado.
11. Pulse **siguiente**. Aparece la página Parámetros del Asistente de enlace de espacio de trabajo.
12. Debe añadir tres símbolos: "taddm_server", "taddm_port" y "taddm_guid". Para añadir un símbolo, realice los pasos siguientes:
    a. Pulse **Añadir símbolo**. Se visualiza la ventana Añadir símbolo.
    b. En el campo **Símbolo**, escriba el nombre del símbolo.
    c. Pulse **Aceptar**.
13. Para cada símbolo que cree, debe enlazarlo a un atributo que represente la columna correcta del informe.
    - Enlace el símbolo "taddm_server" al atributo server de TADDM.
    - Enlace el símbolo "taddm_port" al número de puerto de la consola web de TADDM.

- Enlace el símbolo "taddm_guid" al atributo Component GUID.

Para enlazar un símbolo a un atributo, realice los pasos siguientes:

a. En la página Parámetros del Asistente de enlace de espacio de trabajo, seleccione el símbolo que desee enlazar a una columna de informes.
b. Pulse **Modificar expresión**. Se visualiza la ventana Editor de expresiones.
c. Pulse **Símbolo**. Se visualiza la ventana Símbolos.
d. Navegue hasta el elemento **Atributos**, y seleccione el atributo que desee enlazar al símbolo. Pulse **Aceptar**.
e. En la ventana Editor de expresiones, pulse **Aceptar**. Aparece la página Parámetros del Asistente de enlace de espacio de trabajo.

14. Pulse **siguiente**. Aparece la página de resumen del Asistente de enlace de espacio de trabajo.
15. Pulse **Finalizar**.

Resultados

Si tiene sucesos activos en el informe de sucesos de cambio aparece, junto a cada fila de la tabla, un icono de enlace. Para moverlos al espacio de trabajo de destino, pulse el icono de enlace y seleccione **Mostrar los detalles**. En la fila de la tabla, los valores se sustituyen por símbolos. En el espacio de trabajo, los paneles Historial de cambios y Detalles del objeto se inician en contexto.

Configuración de los sucesos de cambio para un sistema empresarial

Puede utilizar la funcionalidad de sucesos de cambios para enviar un suceso de cambio siempre que se cambie un sistema empresarial.

Acerca de esta tarea

De forma predeterminada, TADDM no indica que un sistema empresarial ha cambiado si una de las máquinas de las que depende ha cambiado.

Procedimiento

Para habilitar el envío de sucesos de cambio para los sistemas empresariales, realice los pasos siguientes:

1. Abra el archivo `$COLLATION_HOME/etc/propagationserver.xml` en un editor apropiado.
2. En la sección Computer System, para los elementos de relación de sistema empresarial y la aplicación, establezca los valores del atributo `enabled` en `true`. Por ejemplo:

```
<relationship enabled="true" source="sys.ComputerSystem" attribute="groups"
target="app.Application" targetAttribute="true"
collectionType="app.FunctionalGroup" radius="1"/>

<relationship enabled="true" source="sys.ComputerSystem" attribute="components"
target="sys.BusinessSystem" targetAttribute="true"/>
```

3. Reinicie TADDM.
4. Cree un escucha para el sistema empresarial, en el archivo de configuración de sucesos de cambio, `$COLLATION_HOME/etc/EventConfig.xml`. En el ejemplo siguiente, el destinatario del suceso es `mycompany-itm`, y el nombre del sistema empresarial es `MyBiz`.

```
<listener object="ITSystem" enabled="true">
 <alert recipient="mycompany-itm"/>
 <attribute name="name" operator="equals">
  <value>MyBiz</value>
 </attribute>
</listener>
```

Planificación de trabajos con IBM Tivoli Workload Scheduler

Puede utilizar IBM Tivoli Workload Scheduler para planificar trabajos en TADDM. IBM Tivoli Workload Scheduler es una herramienta de automatización de software que proporciona la estructura central de la red LAN (backbone) para la gestión y supervisión de carga de trabajo.

Utilice IBM Tivoli Workload Scheduler 8.5.1 o posterior. Debe instalar el gestor de dominio maestro y el agente de tolerancia de errores en el servidor de TADDM. Para obtener más información acerca de cómo instalar y configurar Tivoli Workload Scheduler, consulte http://www-01.ibm.com/support/knowledgecenter/SSGSPN_8.5.1.1/com.ibm.tivoli.itws.doc_8.5.1.1/ic-homepage.html?lang=en. Los objetos de planificación se gestionan con el programa de línea de mandatos del compositor y se almacenan en Tivoli Workload Scheduler.

Los trabajos de Tivoli Workload Scheduler utilizan el script `invokejob.sh` para ejecutar el funcionamiento necesario. El script `invokejob.sh` está proporcionado por la instalación de TADDM.

Los siguientes parámetros son comunes a todos los usos del script:

Necesario: -u *usuario*
: Este valor indica el usuario que ejecuta el mandato de la interfaz de programación de aplicaciones.

Necesario: -p *contraseña*
: Este valor indica la contraseña que autentica el usuario.

Necesario: --profile *perfil*
: Este valor define el perfil de descubrimiento.

Opcional: -H *host*
: Este valor indica el nombre de host del servidor de TADDM. El nombre predeterminado es `localhost`. Si utiliza el parámetro **-T**, debe especificar también el parámetro **-H**.

Opcional: -P *puerto*
: Este valor indica el puerto del servidor de TADDM. El valor predeterminado es `9433`.

Opcional: -v *versión*
: Este valor especifica el nombre o número de versión. El valor predeterminado es `0`.

Opcional: -t *tiempo de espera excedido*
: Este valor especifica la cantidad de tiempo que debe transcurrir antes de que el trabajo se interrumpa automáticamente.

Opcional: -T | --truststorefile *almacén_confianza*
: Este valor especifica la ubicación del archivo de almacén de confianza, `jssecacerts.cert`, con un certificado para la conexión con el servidor de TADDM. Este parámetro es obligatorio para la conexión segura a TADDM. Si utiliza este parámetro, debe especificar también el parámetro **-H**.

Para planificar un trabajo, complete los siguientes pasos:

1. En Tivoli Workload Scheduler, especifique el archivo de definición del trabajo de TADDM en un archivo de edición. El siguiente ejemplo muestra una definición de trabajo como plantilla:

   ```
   WORKSTATION_ID#TADDM_JOB
    SCRIPTNAME "./opt/IBM/taddm/dist/bin/invokejob.sh -u
   ^NOMBREUSUARIO_TADDM^ -p
   ^CONTRASEÑA_TADDM^ mandato [parámetros]"
    STREAMLOGON taddmuser
    TASKTYPE UNIX
    RECOVERY STOP
   ```

   ^*NOMBREUSUARIO_TADDM*^ y ^*CONTRASEÑA_TADDM*^ son variables que deben definirse en Tivoli Workload Scheduler. Estas variables se asignan a los valores que están almacenados en la base de datos. Por razones de seguridad, utilice variables, especialmente al codificar las contraseñas, para asegurar que los valores no sean visibles como texto abierto.
2. Utilice el compositor para añadir el archivo de edición a la base de datos.
3. Añada el trabajo a la secuencia de trabajos y planifique la secuencia de trabajos que va a ejecutar. El agente de IBM Tivoli Workload Scheduler inicia y supervisa la acción del script `invokejob.sh`.

Planificación de un trabajo de descubrimiento

En el siguiente ejemplo se ejecuta un descubrimiento en el ámbito 127.0.0.1:

```
dist/bin/invokejob.sh -u USER -p PASSWORD --timeout 60000 discover start
--profile "Level 3 Discovery" 127.0.0.1
```

En el siguiente ejemplo se ejecuta un descubrimiento del alcance definido de MyScopeSet, que debe existir en la lista de ámbito:

```
dist/bin/invokejob.sh -u USER -p PASSWORD --timeout 60000 discover start
--profile "Level 3 Discovery" MyScopeSet
```

En los ejemplos anteriores, el último parámetro especifica el elemento del ámbito o el ámbito definido que se incluirá en la ejecución del descubrimiento. Es necesario el parámetro **perfil**. El parámetro **nombre**, que es el nombre de la ejecución del descubrimiento es opcional.

El siguiente mandato es un ejemplo de cómo detener un descubrimiento en ejecución:

```
dist/bin/invokejob.sh -u USER -p PASSWORD --timeout 60000 discover stop
```

El mandato **discover stop** no acepta argumentos adicionales.

Planificación de un trabajo de sincronización de dominio

El siguiente ejemplo muestra la sintaxis de la línea de mandatos y las opciones del script de TADDM `invokejob.sh` para ejecutar la sincronización del dominio en un despliegue de servidor de sincronización:

```
dist/bin/invokejob.sh -u USER -p PASSWORD --timeout 60000 sync start TestDomain
```

Los mandatos **sync start** y **sync stop** requieren un argumento, el nombre del dominio para el que iniciar o detener el trabajo de sincronización.

Integración de TADDM con IBM Tivoli Business Service Manager

En función las tareas específicas que deba realizar en su entorno de TI, puede utilizar las prestaciones de integración que están disponibles entre TADDM e IBM Tivoli Business Service Manager. Para utilizar estas prestaciones, debe disponer de IBM Tivoli Business Service Manager 4.2.1 arreglo temporal 3, pero no es necesaria ninguna configuración adicional de TADDM.

Actualización del estado de ciclo de vida para aplicaciones empresariales

Puede utilizar el estado de ciclo de vida para filtrar objetos para su sincronización en IBM Tivoli Business Service Manager desde TADDM. Puede utilizar el programa **BusinessServiceLifecycle** para mostrar información sobre una aplicación empresarial o definir el estado de ciclo de vida de una aplicación empresarial.

La aplicación IBM Tivoli Business Service Manager ITsystems solo incluye aplicaciones empresariales. Por esta razón, el programa **BusinessServiceLifecycle** solo soporta aplicaciones empresariales.

El programa **BusinessServiceLifecycle** está en la siguiente ubicación:

- Para los sistemas operativos Linux y UNIX, el script `BusinessServiceLifecycle` está en el directorio `$COLLATION_HOME/bin`.
- Para los sistemas operativos Windows, el archivo de proceso por lotes `BusinessServiceLifecycle.bat` está en la carpeta `%COLLATION_HOME%\bin`.

Utilice el programa **BusinessServiceLifecycle** con las siguientes opciones de línea de mandatos:

```
BusinessServiceLifecycle -u nombreusuario_TADDM -p contraseña_TADDM -l | -s
identificador exclusivo global estado
```

Utilice la opción `-l` para mostrar información del ciclo de vida de la aplicación empresarial o utilice la opción `-s`, junto con un parámetro guid y un parámetro de código de estado, para definir un estado de ciclo de vida. No puede utilizar la opción `-l` y la opción `-s` al mismo tiempo.

La siguiente tabla muestra los códigos de estado válidos:

Tabla 49. Códigos de estado

Código	Estado
0	Desconocido
1	Otro
2	Pedido
3	Recibido
4	En prueba
5	Probado
6	Instalado
7	Habilitado
8	Inhabilitado
9	Mantenimiento
10	Retirado

Tabla 49. Códigos de estado (continuación)

Código	Estado
11	Archivado
12	Aceptado
13	En compilación
14	En desarrollo
15	Borrador
16	Inventario
17	Fuera de línea
18	Postproducción
19	Producción
20	Listo para producción
21	En fase de terminación
22	En validación

Integración de TADDM con Jazz for Service Management

TADDM admite la integración con plataformas de Open Services for Lifecycle Collaboration (OSLC). OSLC, si se utiliza con TADDM, le permite obtener los datos de descubrimiento presentados con el formato de definiciones de recurso estándar. La plataforma Jazz for Service Management es una herramienta de integración de IBM basada en especificaciones de comunidad abierta de OSLC.

Jazz for Service Management ofrece un único punto de configuración y administración de productos Tivoli, entre otros. Jazz for Service Management muestra una visión global de las relaciones empresariales, de aplicaciones y de recursos de TI.

Comunicación REST OSLC de TADDM

El servicio REST (Representational State Transfer) de TADDM proporciona integración con OSLC en varios canales de información REST de OSLC. El servicio especifica los tipos de soporte que se devuelven durante la ejecución y describe los aspectos de seguridad conectados al servicio.

CRTV (vocabulario de tipo de recurso común) es un modelo de datos definido por IBM y la comunidad OSLC admitido por TADDM, junto con Tivoli Common Data Model (CDM). El soporte de TADDM para OSLC hace que los datos de descubrimiento de CDM pasen a estar disponibles como recursos definidos por CRTV.

Interfaz REST de OSLC:

Hay una interfaz REST disponible en TADDM for Open Services Lifecycle Collaboration (OSLC). Puede utilizar la interfaz REST de OSLC para obtener información sobre elementos de configuración (CI) registrados, sus atributos y su historial de cambios.

Puede obtener información sobre los atributos del elemento de configuración solo si el CRTV (vocabulario de tipo de recurso común) o el vocabulario de TADDM admiten dichos atributos.

Todas las solicitudes válidas deben tener un identificador exclusivo global que identifique el elemento de configuración concreto.

Hay dos tipos de servicio:

Servicio de configuración
Este servicio proporciona una interfaz para recuperar atributos ampliados para un recurso de CRTV.

Servicio del historial de cambios
Este servicio proporciona una interfaz para recuperar el historial de cambios de un período de tiempo especificado para un recurso de CRTV.

Por cada servicio, puede ver los tres tipos de contenido siguientes:

- Representación de RDF
- Vista compacta de OSLC
- Vista previa HTML

El URL siguiente es la dirección base:

`http[s]://host_taddm:puerto/cdm/oslc/nombre_proveedor/guid_ci`

donde

- *puerto* es el puerto donde escucha el servidor Tomcat (TADDM 7.3.0) o el servidor de perfil WAS Liberty (TADDM 7.3.0.1 y posterior). El valor predeterminado es 9430.
- *nombre_proveedor* es uno de los dos valores siguientes, según el servicio que quiera utilizar:
  - `configuration`
  - `changehistory`
- *guid_ci* es el ID del elemento de configuración en TADDM

Para obtener la vista previa HTML de un elemento de configuración, utilice el URL siguiente:

- `http[s]://host_taddm:puerto/cdm/oslc/nombre_proveedor/guid_ci/preview`

La interfaz REST de OSLC solo acepta solicitudes HTTP-GET. Puede utilizar la cabecera HTTP Aceptar para especificar el tipo de contenido devuelto.

Para obtener la vista compacta de OSLC del elemento de configuración dado, especifique la siguiente cabecera Aceptar:

`application/x-oslc-compact+xml`

Para obtener la representación RDF del elemento de configuración dado, especifique la cabecera Aceptar:

`application/rdf+xml`

Es el comportamiento predeterminado si no se proporciona ningún valor para la cabecera Aceptar.

Vista compacta de OSLC:

La vista compacta de OSLC es una representación XML de un recurso de destino.

La vista compacta de OSLC es una vista previa proporcionada por la interfaz REST de OSLC. Para obtener una vista previa de un recurso de destino, el proveedor debe proporcionar una representación de los recursos, según se ha definido en la especificación de OSLC.

Puede obtener esta representación del recurso utilizando una solicitud HTTP GET con el URI del recurso de destino, junto con la cabecera de acceso `application/x-oslc-compact+xml`.

Si el proveedor admite el mecanismo de vista previa, responderá con una representación compacta que incluye información que el consumidor puede utilizar para visualizar enlaces y una vista previa del recurso de destino.

Vista previa HTML de Jazz for Service Management:

Jazz for Service Management Registry Services proporciona una interfaz de usuario HTML para ofrecer información sobre elementos registrados desde sistemas externos conectados.

Todos los elementos que tienen datos proporcionados por TADDM disponen de una vista previa HTML que proporciona una rápida visión general de los datos del elemento seleccionado, directamente desde el servidor de TADDM.

TADDM proporciona Jazz for Service Management con un servicio de información en la dirección siguiente:

`http[s]://`*`nombre_host`*`:`*`puerto`*`/cdm/oslc/configuration/`*`guid`*`/preview`

donde *nombre_host* y *puerto* son el nombre de host y el número de puerto del servidor de TADDM y *guid* es el identificador exclusivo del elemento.

El URL muestra una página con información de visión general sobre el elemento seleccionado. La página se visualiza automáticamente en la interfaz de usuario Jazz for Service Management.

El contenido de la página es parecido al del separador General en la vista Detalles de resumen del inventario disponible en Data Management Portal de TADDM.

Seguridad:

Puede configurar TADDM de tal modo que el acceso a los canales de información proporcionados por la interfaz REST de OSLC requiera autenticación.

Para acceder a la interfaz REST, tiene que autenticarse utilizando uno de los métodos siguientes:

Autenticación HTTP básica
: Las credenciales se deben colocar en la cabecera de petición de autorización. El valor de dicha cabecera debe respetar las reglas de la autenticación HTTP básica.

Inicio de sesión único
: Si utiliza el inicio de sesión único, todas las solicitudes enviadas a la interfaz REST tienen que ir acompañadas de una señal de Lightweight Third-Party Authentication (LTPA). Para verificar la señal, TADDM debe haberse configurado para utilizar WebSphere Virtual Member Manager (VMM) como repositorio de usuarios.

Para obtener más información sobre cómo configurar VMM, consulte "Configuración del servidor de TADDM para utilizar repositorios federados de WebSphere" en la página 27.

Para proporcionar las fuentes solicitadas y presentarlas sin autenticación, la siguiente propiedad del archivo `collation.properties` debe configurarse con un URL de servicios de registro válido:

`com.ibm.cdb.topobuilder.integration.oslc.frsurl`

A continuación se utilizan un nombre de usuario y una contraseña configurados previamente si no se incluyen credenciales válidas con la solicitud.

El nombre de usuario y la contraseña se toman del archivo de descriptor de despliegue `web.xml` de la aplicación web Common Data Model. Puede configurar esta personalización utilizando los siguientes parámetros init de OSLCFilter:

OSLC_LOGIN_OFF
Si este parámetro se establece en `true`, el nombre de usuario y la contraseña especificados por los parámetros OSLC_USER y OSLC_PASSWORD se utilizan en el caso de que las solicitudes entrantes no contengan sus propias credenciales válidas.

Si este parámetro se establece en `false`, la solicitud entrante tiene que contener credenciales válidas.
El valor predeterminado es `true`.

OSLC_USER
Este parámetro está establecido en el nombre de usuario que se utiliza si no se incluyen credenciales válidas con la solicitud. Si es necesario, puede cambiar el nombre de usuario utilizado.

El valor predeterminado es `administrator`.

OSLC_PASSWORD
Este parámetro está establecido como la contraseña que se utiliza si no se incluyen credenciales válidas con la solicitud. Si cambia la contraseña del administrador utilizando la IU de TADDM, tiene que actualizar el valor de la contraseña definido por este parámetro.

El valor predeterminado es `collation`.

Exportación de datos a los servicios de registro mediante OSLCAgent

Puede utilizar el agente de topología OSLCAgent para exportar información sobre elementos de configuración a los servicios de registro.

OSLCAgent es una solución automatizada para exportar datos de TADDM a los servicios de registro. El agente realiza periódicamente las tareas siguientes:

- Consultas de objetos que se pueden registrar en los servicios de registro
- Convertirlas en mensajes con formato RDF
- Publicarlas mediante HTTP

OSLCAgent pertenece al grupo de integración. El intervalo de tiempo entre ejecuciones se especifica en la entrada siguiente del archivo `collation.properties`:

`com.ibm.cdb.topobuilder.groupinterval.integration`

OSLCAgent puede actuar como proveedor de configuración y proveedor del historial de cambios. Estas dos funciones se pueden habilitar por separado. Para habilitar la función del proveedor de configuración, defina la siguiente propiedad en `true`:

`com.ibm.cdb.topobuilder.integration.oslc.enable.configurationsp`

Para habilitar la función del proveedor de historial de cambios, defina la siguiente propiedad en `true`:

`com.ibm.cdb.topobuilder.integration.oslc.enable.changehistorysp`

Para configurar OSLCAgent de manera que se conecte a los servicios de registro, es necesario especificar la dirección de los servicios de registro y acceder a los detalles de entrada.

Configure la dirección de los servicios de registro en la propiedad siguiente:

`com.ibm.cdb.topobuilder.integration.oslc.frsurl`

Especifique la dirección de los servicios de registro con el formato siguiente:

protocolo`://`*nombre_host_o_ip_o_fqdn*`:`*puerto*

Por ejemplo, `http://192.0.2.24:9081`

Nota: Se prefieren el nombre de dominio totalmente calificado (FQDN) o el nombre de host totalmente calificado a la dirección IP para proporcionar coherencia con otros productos y evitar problemas de integración. No obstante, si los demás productos que se utilizan con TADDM utilizan la dirección IP, debe especificar la dirección IP. Si no se utiliza ningún producto con TADDM, es preferible utilizar FQDN en el caso de que se añadan más adelante otros productos.

Cree una entrada de lista de acceso de tipo **Servicio de registro/integración**. Especifique el nombre de usuario y la contraseña para los servicios de registro.

Puede ajustar el funcionamiento de OSLCAgent utilizando las propiedades siguientes:

com.ibm.cdb.topobuilder.integration.oslc.maxtimeperrun
: Esta propiedad especifica el tiempo máximo (en minutos) durante el que se puede ejecutar OSLCAgent. Los proveedores pueden superar este tiempo en la misma medida que el tiempo consumido por los trabajos enviados a la agrupación antes de que se agote el tiempo. Si la propiedad no se ha configurado o se ha establecido en `-1`, el tiempo permitido para una única ejecución de OSLCAgent es ilimitado.

com.ibm.cdb.topobuilder.integration.oslc.jobspoolsize
: Esta propiedad especifica el número máximo de trabajos ejecutándose simultáneamente. Cada trabajo registra un único elemento de configuración. Si la propiedad no está configurada, el valor predeterminado es `10`.

com.ibm.cdb.topobuilder.integration.oslc.frshttptimeout
: Esta propiedad especifica el tiempo de espera en milisegundos para las conexiones HTTP. El valor predeterminado es `5000`.

com.ibm.cdb.topobuilder.integration.oslc.frsfailfastafter
: Esta propiedad especifica el número de tiempos de espera excedidos

consecutivos de la conexión HTTP tras los que un agente considera que los servicios de registro no están disponibles y deja de intentar conectar. El valor predeterminado es 5.

com.ibm.cdb.topobuilder.integration.oslc.unregisterableIPs
Esta propiedad especifica las direcciones IP que no se deben registrar, ya que no son públicas y es posible que provoquen una sobrefusión de los registros de recurso. Esta propiedad puede contener expresiones regulares. El valor predeterminado es
`127.0.0.1,0111111100000000000000000000001,0:0:0:0:0:0:0:1,`
`000000000000000000000000000000000000000000000000000000000000`
`000000000000000000000000000000000000000000000000000000000000`
`000000000001`.

com.ibm.cdb.topobuilder.integration.oslc.unregisterableFQDNs
Esta propiedad especifica nombres de dominio completos que no se deben registrar, ya que no son públicos y es posible que provoquen una sobrefusión de los registros de recurso. Esta propiedad puede contener expresiones regulares. El valor predeterminado es
`localhost.localdomain,localhost,loopback6(.?\u005c\w*)*`.

com.ibm.cdb.topobuilder.integration.oslc.enablecrtvtype.*TipoCRTV*
Esta propiedad especificar que OSLCAgent procesa únicamente elementos de configuración de un tipo concreto de CRTV (vocabulario de tipo de recurso común). Si está habilitada, solo se registrarán y actualizarán los elementos de configuración de dicho tipo de CRTV, y solo estos registros serán anulados.

Por ejemplo, si define

```
com.ibm.cdb.topobuilder.integration.oslc.enablecrtvtype.ComputerSystem=true
```

, especifica que solo se procesan los sistemas informáticos.

Se permiten los tipos de CRTV siguientes:

- ComputerSystem
- Database
- Fix Pack 2 SAPSystem
- ServiceInstance
- SoftwareModule
- SoftwareServer

com.ibm.cdb.topobuilder.integration.oslc.history.days_previous
Esta propiedad especifica el número de días de información de historial de cambios disponible utilizando el URL de iniciar en contexto (LIC). El valor predeterminado es 5.

Puede utilizar la propiedad `days_previous` para controlar la cantidad de espacio de almacenamiento y el tiempo de proceso necesarios para gestionar la información de historial de cambios.

El URL de LIC se lista en la vista previa HTML del historial de cambios de OSLC.

Si el valor es mayor que 0, el parámetro `days_previous` se aplica al URL de LIC para limitar la cantidad mostrada del historial de cambios.

Si el valor es igual o menor que 0, el URL de LIC no contiene el parámetro `days_previous` y puede ver todo el historial de cambios de ese CI.

Interfaz de línea de mandatos para OSLCAgent

Puede utilizar la interfaz de línea de mandatos (CLI) de OSLCAgent para exportar de forma manual la información sobre elementos de configuración a los servicios de registro.

En el caso de OSLCAgent, puede pasar una combinación de mandatos y conmutadores al script `runtopobuild` o al archivo de proceso por lotes. Cada mandato y conmutador tiene un formato corto de una sola letra y un formato descriptivo más largo. Puede utilizar cualquier combinación de formatos de mandato y conmutador.

Los mandatos disponibles son los siguientes:

- `-R | –refreshAll true|false`

  Este mandato registra todos los elementos de configuración elegibles, aunque se hayan registrado ya.
- `-r | -refreshGuid` *`GUID`*

  Este mandato registra el elemento de configuración que tenga el GUID (identificador exclusivo global) especificado, aunque se haya registrado ya.
- `-l | -refreshIgnored true|false`

  Si se descubre un elemento de configuración en una posición sin suficiente profundidad, puede que este no tenga reglas de denominación con el formato correcto. De forma predeterminada, OSLCAgent ignora dichos elementos de configuración. Este mandato fuerza al OSLCAgent a volver a procesar esos elementos de configuración.

Para especificar acciones concretas, puede pasar un conmutador con cualquier mandato. Hay dos tipos de conmutador disponibles.

Puede utilizar los conmutadores siguientes para habilitar o inhabilitar el proceso de determinados tipos de CRTV:

- `-c | --enableComputerSystem true|false`
- `-d | --enableDatabase true|false`
- `-i | --enableServiceInstance true|false`
- `-m | --enableSoftwareModule true|false`
- `-s | --enableSoftwareServer true|false`

Por ejemplo, si no desea volver a registrar sistemas informáticos, utilice los conmutadores `-c false`.

Puede utilizar los conmutadores siguientes para habilitar o inhabilitar los roles de configuración e historial de cambios.

- `-h | --enableChangeHistoryProvider true|false`
- `-p | --enableConfigurationProvider true|false`

Por ejemplo, si no desea que realizar un nuevo registro como un proveedor de historial de cambios, utilice los conmutadores `-h false`.

Si desea utilizar los valores predeterminados en caso de no pasar un mandato o un conmutador al ejecutar el script `runtopobuild` o el archivo de proceso por lotes, configure las siguientes propiedades en el archivo `collation.properties`:

- `com.ibm.cdb.topobuilder.integration.oslc.refreshAll=true|false`
- `com.ibm.cdb.topobuilder.integration.oslc.refreshGuid=`*`GUID`*

- com.ibm.cdb.topobuilder.integration.oslc.enablecrtvtype.*tipo_crtv*

Para obtener una lista completa de los parámetros y conmutadores disponibles, vaya a $COLLATION_HOME/support/bin y ejecute el script runtopobuild o el archivo de proceso por lotes con el conmutador -H. Por ejemplo,

```
./runtopobuild.sh -H
```

Registro de elementos de configuración con los servicios de registro

En este tema se muestran los elementos de configuración descubiertos por TADDM a los que se solicita un registro en los servicios de registro y los atributos que se definen, así como información detallada sobre correlaciones.

Si un elemento de configuración concreto no se ha registrado, las hebras de registro producirán información de registro sobre el motivo por el cual no se ha registrado el elemento de configuración. La lista de atributos de regla de denominación no definidos se muestra en el registro. Para configurar el nivel de registro correcto, defina el siguiente valor de propiedad en el archivo collation.properties:

```
com.collation.log.level.vm.Topology=DEBUG
```

Los atributos siguientes son comunes para todos los tipos de CRTV:

Guid Establezca el valor de GUID del CI.

name Establezca el valor de los atributos name, label o displayName.

description
Establezca el valor del atributo de descripción.

lastDiscoveredTime
Establezca el valor del atributo lastModifiedTime.

SoftwareServer

El tipo SoftwareServer de CRTV contiene los siguientes atributos y clases de TADDM:

- WebSphereServer
  - host
  - node
  - node.cell
- Db2Instance
  - home
  - host
- MQQueueManager
  - displayName | label | name
- AppServer
  - displayName | label | name
  - host
- CommunityServer
  - displayName | label
- SametimeServer
  - displayName | label

- MeetingServer
  - displayName | label
- SpecialityServer
  - displayName | label | name
- AgentManager
  - displayName | label
- SharePointRole
  - displayName | label | name

Los atributos de TADDM están correlacionados con los atributos de CRTV de la manera siguiente:

Atributo de TADDM	Atributo de CRTV	Otra información
PrimarySAP	crtv:serverAccessPoint	El recurso serviceAccessPoint se ha registrado, junto con el recurso IpAddress al que señala, utilizando crtv:ipAddress.
version	crtv:version	
vendorName	crtv:manufacturer	
host	crtv:runsOn	crtv:runsOn apunta a ComputerSystem
home	crtv:instancePath	Solo para DatabaseServer y Db2Instance.
dataPath	crtv:instancePath	Solo para MQQueueManager.

rdf:type se ha definido en uno de los valores siguientes:

- `J2EEServer`
- `WebSphereServer`
- `IBMHTTPServer`
- `WebServer`
- `Db2Instance`
- `OracleInstance`
- `MQQueueManager`
- `WebServer`
- `DatabaseInstance`
- `CICSRegion`

ComputerSystem

El tipo ComputerSystem de CRTV contiene los siguientes atributos y clases de TADDM:

- ComputerSystem

  Se ha definido una de las siguientes combinaciones de atributos:
  - systemId &VMID
  - systemId
  - serialNumber & model & manufacturer &VMID
  - serialNumber & model & manufacturer

– systemBoardUUID
– ipInterfaces

Los atributos de TADDM están correlacionados con los atributos de CRTV de la manera siguiente:

Atributo de TADDM	Atributo de CRTV	Otra información
label o displayName	crtv:name	
OSVersion o OSRunning	crtv:version	
hostSystem	crtv:dependsOn	
fqdn	crtv:fqdn	
name	crtv:shortHostname	Si hay un nombre establecido y si se trata de un nombre de host válido. Solo para SunSPARCComputerSystem.
ipInterface	crtv:ipAddress	Todos los FQDN de las direcciones IP se fusionan en crtv:fqdn.

crtv:type se ha definido con uno de los valores siguientes

- `Generic`
- `SunFire`
- `SunSPARC`
- `SystemP`
- `Unitary`
- `Virtual`
- `WPAR`

Para LinuxUnitaryComputerSystem, se correlacionan atributos adicionales del modo siguiente:

Atributo de TADDM	Atributo de CRTV	Otra información
manufacturer	crtv:manufacturer	
model	crtv:model	
serialNumber	crtv:serialNumber	
VMID	crtv:vmid	Si CPUType y Model están definidos: • Para Intel, VMID está definido en `null` y se intenta definir crtv:systemBoardUUID con systemBoardUUID o convertedUUID. • Para la alimentación, se omite CS si tiene VMID definido.

Para SunSPARCUnitaryComputerSystem, se correlacionan atributos adicionales de la misma forma:

Atributo de TADDM	Atributo de CRTV	Otra información
systemId	crtv:hostid	
VMID	crtv:vmid	

Para cualquier otro sistema informático, los atributos adicionales se correlacionan de la siguiente manera:

Atributo de TADDM	Atributo de CRTV	Otra información
manufacturer	crtv:manufacturer	
model	crtv:model	
serialNumber	crtv:serialNumber	
VMID	crtv:VMID	Si OSRunning se establece en `WindowsOperatingSystem`, VMID se define en `null`. Si OSRunning se establece en `HpUx`, los atributos VMID, model y serialNumber se establecen en `null`.
systemBoardUUID o convertedUUID	crtv:systemBoardUUID	
worldWideName	crtv:hostid	Solo para FCSwitch, TapeLibrary y TapeMediaChanger.

Database

El tipo Database de CRTV contiene los siguientes atributos y clases de TADDM:

- Db2Database
  - name | displayName
- IDSDatabase
  - name | displayName
- IMSDatabase
  - name | displayName
- OracleDatabase
  - name | displayName
- SqlServerDatabase
  - name | displayName
- SybaseDatabase
  - name | displayName
- DominoDatabase
  - name | displayName

Los atributos de TADDM están correlacionados con los atributos de CRTV de la manera siguiente:

Atributo de TADDM	Atributo de CRTV	Otra información
name	crtv:name	

Atributo de TADDM	Atributo de CRTV	Otra información
fileName	crtv:name	Solo para DominoDatabase.
parent	crtv:dbInstance	

ServiceInstance

Dependiendo de si la compatibilidad con versiones anteriores está habilitada, el tipo ServiceInstance de CRTV contiene los siguientes atributos y clases de TADDM:

- Cuando la compatibilidad con versiones anteriores está habilitada:
  - BusinessSystem
    - name
  - Application
    - name
  - ServiceInstance
    - name
  - ServiceInfrastructure
    - name
  - SAPSystem
    - SAPSystemSID | systemHome
- Cuando la compatibilidad con versiones anteriores está inhabilitada:
  - CustomCollection (sólo con el tipo "BusinessApplication")
    - collectionId

Los atributos de TADDM están correlacionados con los atributos de CRTV de la manera siguiente:

Atributo de TADDM	Atributo de CRTV	Otra información
name	crtv:name	
SAPSystemSID:systemHome	crtv:name	Si no se han definido name ni displayName. Solo para SAPSystem.
parentGUID o NULL	crtv:parentServiceInstance	
collectionId	crtv:name	

SoftwareModule

El tipo SoftwareModule de CRTV contiene los siguientes atributos y clases de TADDM:

- SoftwareModule
  - fileName
  - name
  - parent.name
- MQQueue
  - name
  - queueManager

Los atributos de TADDM están correlacionados con los atributos de CRTV de la manera siguiente:

Atributo de TADDM	Atributo de CRTV	Otra información
parent	deployedTo	
fileName	crtv:fileName	

rdf:type se establece en uno de los valores siguientes

- `J2EEApplication`
- `MQQueue`

Resolución de problemas de OSLC

En este tema, se describen problemas comunes que se producen con OSLC y se presentan soluciones para dichos problemas.

El URL de TADDM configurado no incluye un número de puerto

Problema

La propiedad URL de TADDM configurada en el archivo `collation.properties`, `taddmURL`, tiene que incluir un número de puerto.

Si la propiedad no se ha configurado con un número de puerto, tiene que actualizar el URL de TADDM para que incluya un número de puerto, borrar la información sobre los servicios de registro o proveedores específicos y borrar las indicaciones de fecha y hora de TADDM.

Solución

Para actualizar el URL de TADDM de modo que incluya un número de puerto, siga estos pasos:

1. En el archivo `collation.properties`, defina la propiedad `taddmURL` de la manera siguiente:

   `taddmURL=http://`*`servidor.dominio:puerto`*

2. En el sistema con servicios de registro, siga estos pasos:
   a. Vaya a `/opt/IBM/JazzSM/registry/etc`.
   b. En el archivo `CLI.properties`, configure las credenciales de las propiedades siguientes:
      - ds.jdbc.user
      - ds.jdbc.password
      - appserver.user
      - appserver.password
   c. Vaya a `/opt/IBM/WebSphere/AppServer/bin`.
   d. ejecute el script `stopServer.sh` para detener el WebSphere Application Server.

      `./stopServer.sh` *`nombre_servidor`* `-user` *`nombre_usuario`* `-p` *`contraseña`*

      por ejemplo,

      `./stopServer.sh server1 -user wasadmin -p passw0rd`
   e. Vaya a `/opt/IBM/JazzSM/registry/bin`.
   f. Ejecute el script `frs.sh` con los parámetros adecuados:

      `./frs.sh uninstall -type db -properties ../etc/CLI.properties`
   g. Asegúrese de que la base de datos se haya soltado. De no ser así, ejecute estos mandatos:

```
db2 drop db nombre_bd
db2 create db nombre_bd
```

donde *nombre_bd* es el nombre de la base de datos de los servicios de registro.

h. Vaya a `/opt/IBM/JazzSM/registry/bin`.

i. Ejecute el script `frs.sh` con los parámetros adecuados:

```
./frs.sh install -type db -properties ../etc/CLI.properties
```

j. Vaya a `/opt/IBM/WebSphere/AppServer/bin`.

k. Ejecute el script `startServer.sh` para iniciar el WebSphere Application Server.

```
./startServer.sh nombre_servidor -user nombre_usuario -p contraseña
```

por ejemplo,

```
./startServer.sh server1 -user wasadmin -p passw0rd
```

l. Ejecute el script `frs.sh` con los parámetros adecuados:

```
./frs.sh uninstall -type container -properties ../etc/CLI.properties
```

m. Ejecute el script `frs.sh` con los parámetros adecuados:

```
./frs.sh install -type container -properties ../etc/CLI.properties
```

Puede eliminar un elemento de los servicios de registro de un proveedor específico con el mandato siguiente:

```
./frs.sh deleteProvider -providerUrl url - properties cli.properties
```

3. En el sistema con la base de datos de TADDM, complete los siguientes pasos:

a. Vaya a `$COLLATION_HOME/support/bin`.

b. Ejecute el script `runtopobuild` o el archivo de proceso por lotes con los parámetros adecuados; por ejemplo:

```
./runtopobuild.sh -a OSLCAgent -R
```

Tivoli Directory Integrator

Al adquirir IBM Tivoli Application Dependency Discovery Manager (TADDM), también recibe Tivoli Directory Integrator, que le permite integrar TADDM con otros orígenes de datos.

Documentación de Tivoli Directory Integrator en Knowledge Center
http://www-01.ibm.com/support/knowledgecenter/SSCQGF_7.1.0/KC_ditamaps/welcome.html?lang=en

Escenarios de integración de TADDM en la wiki de Tivoli Application Dependency Discovery Manager
https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/Integration%20Scenarios

Compatibilidad de entidades empresariales con las versiones anteriores

Se ha introducido una nueva función para permitir la integración entre TADDM y los productos que leen datos en TADDM utilizando DataApi o directamente en la base de datos de TADDM utilizando SQL. Estos productos son, por ejemplo, IBM Tivoli Business Service Manager (TBSM), IBM SmartCloud Control Desk (SCCD) y Tivoli Directory Integrator (TDI). El modelo de datos Business Application actual se basa en la interfaz CustomCollection, que no tiene nada en común con las

interfaces Application y ITSystem anteriores. La nueva función permite la integración con otros productos sin introducir modificaciones en esos sistemas.

En las próximas versiones de TBSM y SCCD, el modelo Business Application se introducirá con características nuevas. El objetivo es generar las entidades empresariales anteriores, que son copias de las instancias de recopilación personalizada.

La nueva función, que proporciona compatibilidad con las versiones anteriores, consta de las siguientes características.

Paso adicional cuando se ejecuta `BizAppsAgent`
: El paso adicional genera entidades empresariales (servicios, aplicación, colección) compatibles con versiones anteriores para cada colección personalizada que genera el agente.

  Para activar este paso, se ha añadido una nueva propiedad al archivo `collation.properties`, `com.ibm.cdb.serviceinfrastructure.earlier.ver.compatibility`. El valor predeterminado de esta propiedad es *TRUE* para el escenario de actualización y *FALSE* para el escenario de nueva instalación.

Soporte de OSLC
: El agente OSLC se ha modificado y puede registrar entidades empresariales antiguas o nuevas colecciones personalizadas. Si el distintivo de compatibilidad está establecido en *TRUE*, se registran entidades empresariales antiguas. De lo contrario, se utilizan colecciones personalizadas para producir un contenido para Jazz for Service Management (JazzSM).

En el futuro, se necesitará una recarga completa de entidades empresariales cuando se integren inicios del producto para cargar datos utilizando nuevos objetos de modelo (colecciones personalizadas y nodos). Las aplicaciones empresariales antiguas (aplicaciones) y las nuevas aplicaciones empresariales (colecciones personalizadas) no pueden tener el mismo GUID. Para evitar duplicados, antes de cargar nuevas colecciones personalizadas, los usuarios deberán eliminar las aplicaciones empresariales antiguas.

Creación de grupos funcionales

Las nuevas aplicaciones empresariales, a diferencia de las aplicaciones empresariales antiguas, no tienen grupos funcionales. No obstante, se ha introducido una nueva funcionalidad de niveles para fines similares. En cada nivel exclusivo, para garantizar la compatibilidad con las versiones anteriores, se crea un grupo funcional con un nombre correspondiente al nombre de nivel.

Para obtener más información, consulte el tema *Niveles de aplicaciones empresariales* en la *Guía de usuario* de TADDM.

Integración de BigFix

Fix Pack 5

IBM ha trabajado en el desarrollo de soporte en TADDM para descubrir máquinas/servidores seguros sin necesidad de usar Anclas y pasarelas, que se basa en la utilización de la infraestructura de BigFix.

Nota: Cada vez que una vía de acceso se muestra como vía de acceso relativa, se supone que es relativa a `$COLLATION_HOME (/opt/ibm/taddm/dist)` o `%COLLATION_HOME% (E:\ibm\taddm\dist)`.

Introducción

IBM/Aricent han trabajado en el desarrollo de soporte en TADDM para descubrir máquinas/servidores seguros sin necesidad de usar Anclas y pasarelas, que se basa en la utilización de la infraestructura de BigFix.

Nota: Cada vez que una vía de acceso se muestra como vía de acceso relativa, se supone que es relativa a `$COLLATION_HOME (/opt/ibm/taddm/dist)` o `%COLLATION_HOME% (E:\ibm\taddm\dist)`.

Finalidad:

TADDM utiliza Anclas y pasarelas para descubrir máquinas/aplicaciones/redes que están detrás del cortafuegos. Actualmente se puede evitar el uso de Anclas y pasarelas utilizando las herramientas de supervisión de IBM Netcool (ITM). De forma alternativa, la integración de TADDM con la arquitectura BigFix se puede utilizar para evitar el uso de anclas y pasarelas. La arquitectura de BigFix se compone del servidor de BigFix (servidor BES) y varios puntos finales de BigFix (clientes BES), donde los clientes de BES son máquinas seguras a las que se puede acceder a través del servidor BES. La infraestructura de BigFix se puede reutilizar/utilizar para ejecutar los paquetes de scripts de TADDM en los clientes BES a través del servidor BES de forma automática.

Las principales ventajas de esta integración para los administradores de TADDM son las siguientes:

1. Capacidad de descubrir zonas de cortafuegos sin anclajes.
2. Capacidad de reutilizar la arquitectura de BigFix (por ejemplo, puertos seguros abiertos) para acceder a puntos finales y ahorrar tiempo de establecimiento para descubrir los mismos destinos utilizando el método de TADDM estándar.
3. Alineación con la dirección estratégica para los sensores basados en script de TADDM.
4. Intervención mínima necesaria del administrador de TADDM.
5. Método alternativo de descubrimiento para máquinas de zonas de cortafuegos sin usar la integración de TADDM e ITM.

Referencia:

Documentación de TADDM

La siguiente tabla muestra las versiones soportadas de los productos con los que TADDM se puede integrar.

Para obtener más información sobre los productos que se integran con TADDM, consulte su documentación:

- Knowledge Center de sensores y TADDM 7.3 (documentación oficial) http://www-01.ibm.com/support/knowledgecenter/SSPLFC_7.3.0/com.ibm.taddm.doc_7.3/welcome_page/kc_welcome-444.html?lang=en
- Sistemas de destino compatibles y sensores de TADDM 7.3 https://www.ibm.com/developerworks/community/groups/service/html/communityview?communityUuid=7d5ebce8-2dd8-449c-a58e-

4676134e3eb8#fullpageWidgetId=Wea1cb2531f10_4ccd_99d7_6ab0334cb21f&file=e70bf323-31f1-45ba-8992-4cb491feab4a

- Configuración del descubrimiento por script asíncrono (ASD) en TADDM https://www.ibm.com/support/knowledgecenter/SSPLFC_7.3.0/com.ibm.taddm.doc_7.3/SensorGuideRef/r_cmdb_async_script_sensors.html#sensorsthatcanbescripted
- Guía de configuración de IBM BigFix https://www.ibm.com/support/knowledgecenter/SSPLFC_7.3.0/com.ibm.taddm.doc_7.3/SensorGuideRef/r_cmdb_async_script_sensors.html#sensorsthatcanbescripted
- Sitio web de soporte de TADDM http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliApplicationDependencyDiscoveryManager.html
- Wiki de TADDM https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/Home Esta es una buena fuente de información actualizada que contiene además las mejores prácticas para TADDM. Añada esta página a sus marcadores.
- Foro de TADDM http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1547&categoryID=15&ca=drs-fo
- Comunidad de solicitudes de mejora http://www.ibm.com/developerworks/rfe/?BRAND_ID=90 En esta comunidad se pueden solicitar mejoras del producto directamente a los desarrolladores de IBM.

Arquitectura de la solución:

La integración de TADDM y BigFix se basa en mejorar y automatizar el comportamiento actual de ASD (descubrimiento por script asíncrono), que requiere la intervención manual del administrador de TADDM. Esta integración utiliza la conectividad que proporciona la infraestructura de BigFix a las máquinas de zonas de cortafuegos para ejecutar el descubrimiento a través de los paquetes de scripts de TADDM.

En ASD, el administrador de TADDM debe llevar a cabo los pasos siguientes manualmente:

1. Ejecutar un script en el servidor de TADDM para crear un paquete de descubrimiento que incluya todos los sensores que se van a ejecutar en el destino.
2. Transferir este paquete al sistema de destino.
3. Ejecutar el paquete de descubrimiento en el sistema de destino.
4. Volver a transferir el archivo resultante generado en el sistema de destino al servidor de TADDM.

Con la solución actual, los pasos manuales se han automatizado y, por lo tanto, la solución también se denomina AASD (descubrimiento de script asíncrono automático). El administrador de TADDM solo tiene que ejecutar un script para iniciar el descubrimiento en el servidor de TADDM y el resto de los pasos se realizarán automáticamente.

Pasos en el descubrimiento de BigFix:

Detalles de los pasos para el descubrimiento de BigFix

Paso 1: script de integración de BigFix

Se ha desarrollado un script “runBigFixDiscovery.sh” que dará inicio al descubrimiento AutoASD (AASD) desde el servidor de descubrimiento de TADDM. El script se puede ejecutar a petición. Este script utiliza el ámbito de descubrimiento y el nombre del perfil de descubrimiento como entradas (además de las credenciales de acceso de BigFix) y da soporte a las siguientes modalidades:

- Modo DESCUBRIMIENTO: para iniciar el descubrimiento de BigFix.
- Modo SONDEO: para el sondeo de los resultados del descubrimiento de BigFix.
- Modo LIMPIEZA: para la depuración a petición de los paquetes resultantes del descubrimiento desde el servidor raíz BES.
- Modo REDESCUBRIMIENTO: para volver a ejecutar el descubrimiento previo.

a) Crear paquete de sensores de AutoASD

- Se utiliza el perfil de descubrimiento especificado para captar la lista de sensores y solo se considera válido un subconjunto de sensores de scripts para la creación del paquete de scripts AASD. Consulte el Apéndice D para obtener una lista completa de los sensores con script compatibles con TADDM, aunque esta característica solo da soporte a un subconjunto de estos sensores, que se admiten en la modalidad ASD estándar.
- Se ignorarán otros sensores sin script en el perfil de descubrimiento.
- El paquete AASD es independiente del SO: como resultado, algunos sensores pueden fallar en puntos finales de BigFix, si no están presentes.
- El paquete de scripts AASD generado se carga en el servidor raíz de BigFix usando la API REST /api/upload.

b) Crear una tarea de BigFix

- El ámbito de descubrimiento especificado se utiliza para crear el XML de “lenguaje de relevancia”, que comprende BigFix.
- El XML de tareas de BigFix se genera con “lenguaje de relevancia” y “lenguaje de scripts de acción” ficticio.
- Se genera el título de tarea según la fecha y hora actual.
- Utilice la API REST /api/tasks/custom/TADDM para crear una tarea de BigFix en el sitio personalizado denominado “TADDM” del servidor de BigFix.

c) Iniciar la tarea de BigFix

- Utilice <SourcedFixletAction> para iniciar la ejecución de la acción de la tarea de BigFix creada anteriormente.
- Se utiliza la API REST de BigFix /api/actions para iniciar la ejecución del “lenguaje de scripts de acción” en el punto final de destino.

Paso 2: ejecución de script

- Como parte de la ejecución del “lenguaje de scripts de acción”, el paquete AASD de TADDM se descomprimirá, y los scripts de sensores incluidos (basados en el perfil de descubrimiento) se ejecutarán en los puntos finales de BigFix.

Paso 3: recopilación de compresión

- Al final de la ejecución del “lenguaje de scripts de acción”, el paquete resultante generado en el cliente BES por la ejecución del paquete AASD de TADDM se copiará al servidor raíz BES.

Paso 4: importación de resultados a TADDM

- TADDM sondeará continuamente la BD del servidor de BigFix para comprobar si el archivo resultante se ha cargado al servidor BES.

- Si la BD muestra que los nuevos archivos resultantes están presentes, TADDM realizará una solicitud HTTP para captar los archivos resultantes cifrados, descifrarlos y guardarlos.
- A continuación, TADDM procesará dichos archivos según el ámbito y el perfil configurados y almacenará los objetos descubiertos en la base de datos.

Integración de TADDM y BigFix (disponibilidad limitada)

El release de disponibilidad limitada de la solución TADDM mejorada para BigFix se centra en la ejecución funcional del descubrimiento de extremo a extremo para Windows, Linux, AIX y Solaris OS y los sensores asociados (para varios puntos finales) y ofrece soporte a la comunicación SSL entre TADDM y BigFix a través de las API REST de BigFix. El descubrimiento se puede iniciar en el servidor de descubrimiento de TADDM y los resultados del descubrimiento se deben recuperar automáticamente y deben ser visibles en la GUI de TADDM.

Asunciones:

Se han tomado en cuenta las asunciones siguientes en la ejecución del descubrimiento:

1. El servidor de BigFix y los clientes cuentan con la versión mencionada en la sección 2.1.

2. Los clientes de BigFix tienen los derechos apropiados para ejecutar el script de tarea/acción de descubrimiento cargado por el servidor de BigFix.

3. El usuario de base de datos SQL de BigFix configurada en collation.properties debe tener acceso de lectura a la base de datos BFEnterprise.

4. Los paquetes de scripts de sensor ejecutados a través de Agentes de BigFix necesitarán acceso de escritura al directorio TEMP configurado (p. ej, "C:\Windows\Temp"). El directorio temporal se puede configurar en collation.properties y se supone que tiene una vía de acceso de directorio sin espacios.

5. La limpieza del paquete de solicitudes de script no se maneja en el servidor de descubrimiento de TADDM y se supone que las gestionará el administrador.

6. Dado que la integración de TADDM y BigFix se basa en la infraestructura de ASD actualmente existente en TADDM, las características de rendimiento de esta integración se basarán en las pruebas de referencia de la infraestructura de ASD.

7. Solo se puede utilizar “taddmusr” para la ejecución del script de descubrimiento de BigFix en el servidor de descubrimiento de TADDM y no se permitirá el usuario root.

8. Limpieza de servidor raíz de BigFix: la limpieza se invocará a cada inicio de TADDM y además se realizará periódicamente según la duración configurada (com.collation.bigfix.root.cleanup.interval = Default 1 day). Esta acción suprimirá los archivos resultantes con más antigüedad que el tiempo configurado (com.collation.bigfix.root.cleanup.days = Default 5 days).

9. Limpieza del servidor de TADDM: se gestionará la limpieza de todos los archivos resultantes creados/copiados en el servidor de TADDM durante el descubrimiento y que contengan el nombre “taddmasd” y acaben por “_DONE”.

(Al menos, debe configurarse un umbral en el punto 6 del Apéndice A para que se habilite la limpieza en el servidor de TADDM).

10. Limpieza de punto final: la limpieza del punto final de descubrimiento está habilitada de forma predeterminada y puede controlarse mediante configuración del parámetro de propiedad siguiente:

- a) "com.collation.bigfix.endpoint.cleanup" establecido en el "N" inhabilitará la limpieza en el punto final de descubrimiento.

Requisito previo:

Antes de iniciar el descubrimiento desde el servidor de TADDM, deben cumplirse los siguientes requisitos previos:

1. Es obligatorio seleccionar ASDSensor, ASDPingSensor y el sensor de servidor genérico y desmarcar PingSensor, PortSensor y SessionSensor durante la creación del perfil de descubrimiento.

2. Se han completado todos los pasos de configuración de la sección 2.3.

3. El script de acción de BigFix ha utilizado el mandato powershell nativo para descomprimir el paquete de solicitudes en el punto final de Windows y el mandato tar nativo en Linux.

Nota: Basado en requisitos específicos, se puede personalizar el lenguaje de scripts de acción. Se da soporte a esta personalización con la actualización del archivo modificable del cliente ActionScript_Pre_Post.txt, que se encuentra en la carpeta `$COLLATION_HOME/etc/`; por ejemplo, para habilitar la descarga y el uso de software de descompresión personalizado (la distribución del ejecutable se encuentra en el servidor raíz de BigFix). A continuación, se proporciona un ejemplo de fragmento de código de muestra:

```
%WIN_PRE_START%
if {not exists file "C:\Windows\System32\unzip.exe"}
prefetch unzip.exe sha1:e1652b058195db3f5f754b7ab430652ae04a50b8
size:167936 http://10.160.161.199:52311/Uploads/Unzip/unzip.exe

// Asegúrese de que el entorno se ha establecido correctamente y que la utilidad "unzip"
está disponible en la VÍA DE ACCESO de Windows
copy "__Download\unzip.exe" "C:\Windows\System32\unzip.exe"

endif
%WIN_PRE_END%

%WIN_POST_START%
%WIN_POST_END%

%LIN_PRE_START%
%LIN_PRE_END%
...
```

4. El usuario que ejecuta el descubrimiento debe tener permisos de lectura/escritura en la carpeta resultante.

5. Debe haber suficiente espacio de disco, capacidad de proceso y memoria para atender a las solicitudes y paquetes de resultados que se procesan en el servidor TADDM, servidor raíz de BigFix y destino de descubrimiento.

6. Debe configurarse el Agente de BigFix (sistema de punto final) con un valor suficiente para que el parámetro "_BESClient_ArchiveManager_MaxArchiveSize" habilite cargas de resultados correctas en el servidor raíz de BigFix.

7. Debe establecer un perfil y un ámbito correctos (consulte la sección 4.1 para definir el ámbito y el perfil).

8. Debe configurarse el nombre de sitio "TADDM" y debe estar presente en el servidor de BigFix.

9. Todos los requisitos previos necesarios para los scripts de sensor ASD estándar son aplicables también en caso de descubrimiento de BigFix.

- a) El ejecutable de Powershell debe estar instalado y configurado correctamente en caso de que se realice un descubrimiento que implique el punto final de Windows2003.

Limitaciones:

Las limitaciones siguientes se asocian al release actual:

1. Los destinos de descubrimiento especificados durante el descubrimiento y no accesibles desde el servidor raíz de BigFix no estarán visible en el historial de descubrimientos.

2. PingSensor, PortSensor y SessionSensor se habilitan automáticamente cuando se eligen y habilitan otros sensores, y estos se deben inhabilitar manualmente durante la creación del perfil de descubrimiento.

3. La limpieza del paquete de solicitudes en el servidor raíz de BigFix/servidor de descubrimiento de TADDM no es compatible por diseño. Es posible que se utilice durante el redescubrimiento (desencadenado por la modalidad de redescubrimiento).

4. El redescubrimiento solo se admite desde el mismo servidor de descubrimiento de TADDM en el que se inició el descubrimiento original.

5. Este es el release de disponibilidad limitada y, por lo tanto, la traducción, el soporte de documentación en línea, etc. no están disponibles.

6. El descubrimiento de servidores personalizados no se admite en la integración de BigFix.

Configuración:

Siga los pasos mencionados en esta sección para establecer la configuración deseada.

Configuraciones básicas para el descubrimiento de BigFix:

1. Defina las siguientes propiedades obligatorias en $COLLATION_HOME/etc/collation.properties

a) Valores de la característica de integración de BigFix

```
com.collation.bigfix.enabled=true
```

b) Valores del servidor de BigFix

- com.collation.bigfix.host=<IP o FQDN del servidor de BigFix>
- com.collation.bigfix.port=<Núm_puerto>
- com.collation.bigfix.uid=<Id_usuario de acceso a la consola del servidor de BigFix>
- com.collation.bigfix.pwd=<Contraseña de acceso a la consola del servidor de BigFix>

c) Valores de BD de BigFix

- com.collation.bigfix.db.type=<MSSQL/DB2>
- com.collation.bigfix.db.host=<IP o FQDN de la BD del servidor de BigFix>
- com.collation.bigfix.db.port=<Puerto en el que TADDM se conectará a la BD de BigFix>
- com.collation.bigfix.db.dbname=<Nombre de la BD de BigFix>
- com.collation.bigfix.db.domain=<Dominio de usuario> Parámetro opcional: solo necesario cuando se configura la autenticación basada en Windows para la BD de BigFix>
- com.collation.bigfix.db.uid=<ID de usuario de acceso a la BD de BigFix>
- com.collation.bigfix.db.pwd=<Contraseña de acceso a la BD de BigFix>

d) Valores de hebra de proceso resultante

- com.ibm.cdb.discover.asd.ProcessUnreachableIPs=true
- com.ibm.cdb.discover.asd.autodiscovery.enabled=true

2. Defina las propiedades siguientes en $COLLATION_HOME/etc/ collation.properties, solo si la configuración de SSL está habilitada en el servidor de BigFix:

e) Certificado de BigFix

- com.collation.bigfix.certificate.type=<PKCS12/JKS>
- com.collation.bigfix.certificate.file=<Vía de acceso completa al archivo de certificado>
- com.collation.bigfix.certificate.pwd=<Contraseña para utilizar el certificado>

Nota: Hay más propiedades aparte de las obligatorias que se pueden configurar. Consulte el Apéndice A para obtener una lista completa de las propiedades y sus detalles.

Nota: No se admite el certificado generado con la contraseña en blanco.

3. Ejecute el script “encryptprops.sh” para cifrar las propiedades (consulte el Apéndice C para comprobar el formato de la ejecución de este script). De lo contrario, los scripts de descubrimiento (runBigFixDiscovery.sh/.bat) fallarán con un error de falta de argumentos o argumentos no válidos (consulte el Apéndice E para obtener detalles del código de error), ya que no se aceptan las contraseñas no cifradas.

4. Cree la carpeta $COLLATION_HOME/var/asdd para almacenar los archivos resultantes en TADDM. Si la carpeta var/asdd no se va a utilizar, la propiedad "com.ibm.cdb.discover.asd.AsyncDiscoveryResultsDirectory" debe establecerse con una carpeta específica en la que el administrador desea que se descarguen los archivos resultantes.

5. Reinicie TADDM.

6. Cree un perfil de descubrimiento con los sensores necesarios que se listan en la sección 2.1. El perfil debe tener los sensores obligatorios, además de otros sensores que se están descubriendo.

7. Cree un ámbito de descubrimiento con los puntos finales de destino de BigFix en los que se debe ejecutar el descubrimiento.

Otra configuración:

En un servidor de BigFix, se va a crear un nombre de sitio denominado "TADDM".

1. Abra la "consola de BigFix" y > vaya al separador "Herramientas" -> seleccione "Crear sitio personalizado" -> indique el nombre de sitio "TADDM".

2. Haga clic en "TADDM" -> seleccione el separador "Suscripciones del sistema" -> suscríbase a los sistemas según el requisito (debería incluir todos los sistemas a los que el servidor de BigFix debe conectarse a través de TADDM).

Archivo de registro y sugerencias para la resolución de problemas:

En caso de que se encuentre alguna anomalía durante el descubrimiento, se puede comprobar lo siguiente. Confirme que se cumplen y siguen todos los requisitos previos:

Servidor de descubrimiento de TADDM

- Para comprobar los registros de la ejecución de scripts de descubrimiento de BigFix
  - `$COLLATION_HOME/log/BigFixDiscovery.log`
- Para comprobar en los registros si el archivo resultante accede al servidor de TADDM o no:
  - `$COLLATION_HOME/log/services/ApiServer.log` (busque las palabras clave 'BigfixDiscoveryServerController' y 'AASDiscoveryServerController')

Servidor raíz de BigFix

Para comprobar el estado del descubrimiento y la ejecución de acción usando `IBM BigFix Console` en el **servidor raíz de BigFix**

1. Abra **IBM Bigfix Console**.
2. Seleccione **Sitio** (Personalizar->TADDM) -> **Fixlets** y **Tareas**.
3. Seleccione **Tarea** (dada durante la ejecución de script).
4. Revise **Detalles** e **Historial de acciones**.
5. Seleccione el **Historial de acciones particular** -> **Sistemas informados**.
6. Compruebe el estado y para la ejecución por líneas **efectúe una doble pulsación**.
7. Pulse **Aceptar** para volver a la ventana Perfiles de descubrimiento.

Agente de BigFix/Destino de descubrimiento

- Compruebe que el archivo resultante esté presente en la carpeta `%wintemp%"/taddm7.3.0.4/asd` (solo cuando la propiedad com.collation.bigfix.endpoint.cleanup esté establecida en "N").

- Se puede hacer referencia al archivo `allErrors.txt` (presente en `%wintemp%"/taddm7.3.0.4/asd`) para ver si hay errores durante la ejecución del script de los sensores.

Ejecución del descubrimiento de Bigfix:

Ejecución del descubrimiento de Bigfix

Creación de ámbitos:

Abra la GUI del servidor de TADDM para crear un ámbito de descubrimiento. El ámbito debería incluir todos los puntos finales de destino de BigFix. Los puntos finales de destino se pueden definir como hosts individuales o especificando un rango de redes/dominios.

Creación de perfil:

Se debe crear un perfil de descubrimiento mediante la GUI del servidor de TADDM. Este perfil debe incluir los sensores para las aplicaciones que el administrador desea descubrir mediante TADDM. Consulte la sección 2.1 para obtener más información sobre los sensores que deben incluirse/excluirse obligatoriamente en el perfil de descubrimiento creado.

Ejecución de script:

Para ejecutar el descubrimiento, el script "runBigFixDiscovery.sh" se debe ejecutar desde $COLLATION_HOME/bin. El script se puede ejecutar en 4 modalidades "descubrimiento", "sondeo", "limpieza" y "redescubrimiento". En la modalidad de descubrimiento, se inicia el descubrimiento. En la modalidad de sondeo, se captará el estado de descubrimiento actual. En la modalidad de limpieza, se desencadenará la limpieza de los archivos resultantes en el servidor raíz de BigFix y en la modalidad de redescubrimiento, el descubrimiento ejecutado anteriormente se podrá ejecutar de nuevo.

1. Modalidad de descubrimiento

TADDM proporciona Jazz for Service Management con un servicio de información en la dirección siguiente:

```
./runBigFixDiscovery.sh -d -o <dir salida> -s <ámbito> -p <perfil>
Donde,
-d – para la modalidad de descubrimiento
-o - directorio de salida donde se crearía el paquete de descubrimiento
-s – ámbito de entrada, con los puntos finales de destino de BigFix que se han de descubrir
-p – perfil de entrada, con los sensores que se van a ejecutar
```

Una vez que el mandato se ejecuta en modalidad de descubrimiento, se inicia el descubrimiento. Esto le mostrará el estado de los pasos realizados y le dará un ID de "Acción". Esta acción se puede utilizar en la modalidad de sondeo para comprobar el estado de la acción en cada punto final de BigFix.

Nota:

- El “ID de acción” creado para el descubrimiento (que se muestra en la salida de la consola, p. ej., 2090 en el ejemplo siguiente) se puede reutilizar para el sondeo.

- Mantenga el nombre de la tarea de BigFix creada (que se muestra como "NombreTarea" en la salida de la consola, p. ej. 20180130125432) asociado al ámbito y perfil determinados, que se puede utilizar para el redescubrimiento.

2. Modalidad de sondeo

```
./runBigFixDiscovery.sh -p -r <repetición> -i <ID de acción>

Donde,
-p – para la modalidad de sondeo
-r – núm. de veces que se realizará el sondeo en el servidor de BigFix
-i - ID de acción obtenido del mandato de modalidad de descubrimiento
```

3. Modalidad de limpieza

```
./runBigFixDiscovery.sh -c -d <núm. de días>
Donde,
-c – para la modalidad de limpieza
-d – se van a eliminar los archivos anteriores al número de días especificado
```

4. Modalidad de redescubrimiento

```
./runBigFixDiscovery.sh  -r/--rediscover -i <NombreTarea>
Donde,
-r – para la modalidad de redescubrimiento
-i – NOMBRE DE TAREA correspondiente al descubrimiento anterior que se va a volver a ejecutar
```

Nota: En el Apéndice B se ofrecen más detalles sobre este mandato con todas las opciones posibles y en el Apéndice C se puede consultar un ejemplo para ejecutar el mandato.

Proceso de resultados de descubrimiento:

La modalidad de sondeo del mandato "runBigFixDiscovery.sh" proporciona el estado de la acción ejecutada en cada punto final de BigFix. Basándose en el estado, se creará y procesará el archivo resultante.

1. Una vez completada la acción satisfactoriamente para el punto final, se descargará un archivo resultante para ese punto final en la carpeta resultante configurada (de forma predeterminada, es var/asdd. Consulte la sección 2.3.1 para más información sobre la configuración de la carpeta resultante).

2. Una vez completada la acción satisfactoriamente para el punto final, se descargará un archivo resultante para ese punto final en la carpeta resultante configurada (de forma predeterminada, es var/asdd. Consulte la sección 2.3.1 para más información sobre la configuración de la carpeta resultante).

3. Una vez que los archivos resultantes se procesan satisfactoriamente, el resultado puede estar disponible en la GUI de TADDM, en el separador Historial.

4. Los datos resultantes procesados se almacenarán en la base de datos de TADDM y estarán disponibles en el Portal de gestión de datos o en el PSS de TADDM.

Posible escenario de anomalía:

En caso de que se encuentre alguna anomalía durante el descubrimiento, el sondeo, la limpieza o el redescubrimiento, se puede comprobar lo siguiente:

1. Confirme que se siguen todos los requisitos previos mencionados en la sección 2.2:

2. Compruebe los registros de TADDM en la vía de acceso:

- `$COLLATION_HOME/log/BigFixDiscovery.log`: para los registros de ejecución de script y descubrimiento
- `$COLLATION_HOME/log/services/ApiServer.log`: para los registros de análisis y captación resultantes

3. Consulte los registros de servidor de BigFix y la consola de BigFix para saber si existe algún estado de anomalía.

4. Los registros de ejecución del **lenguaje de scripts de acción de Bigfix** se podrían verificar si el **sondeo de acciones** obtiene un error del **servidor raíz** y el **punto final**.

Apéndice A. collation.properties utilizadas en la integración

1. Función de BigFix habilitada

Tabla 50.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.enabled	true/false	Si es true, la función BigFix se habilitará. Después de establecer esta propiedad en true, se necesita el reinicio de TADDM.	S

2. Servidor de BigFix

Tabla 51.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.host	IP o FQDN	IP o FQDN del servidor de BigFix.	S
com.collation. bigfix.port	<núm. de puerto> Predeterminado=52311	Puerto al que TADDM enviará la solicitud al servidor de BigFix.	N
com.collation. bigfix.uid	<IDusuario>	ID de usuario para acceder a la consola del servidor de BigFix.	S
com.collation. bigfix.pwd	<contraseña>	Contraseña para acceder a la consola de servidor de BigFix. Se almacenará en formato cifrado.	S
com.collation. bigfix.connectTo	<periodo_tiempo> Predeterminado=20 s	TADDM esperará este periodo en segundos antes del tiempo de espera de conexión HTTP/RestAPI.	N
com.collation. bigfix.responseTo	<periodo_tiempo> Predeterminado=20 s	TADDM esperará este periodo en segundos antes del tiempo de espera de respuesta HTTP.	N

Tabla 51. (continuación)

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.site.type	<tipo_sitio> Predeterminado=custom	Tipo del sitio en el servidor de BigFix con el que se conectará TADDM.	N
Visibility.Control. Automation	<nombre_sitio> Predeterminado=TADDM	Nombre del sitio en el servidor de BigFix con el que se conectará TADDM.	N
com.collation. bigfix. aasdpkgmaxsize	<tamaño del paquete de solicitudes> Predeterminado=1024	Tamaño máximo del paquete de solicitudes permitido generado por el script de descubrimiento de BigFix.	N

3. Certificado del servidor de BigFix

Tabla 52.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.certificate.type	<PKCS12/JKS> Predeterminado=JKS	Tipo de certificado de cliente soportado.	N
com.collation. bigfix.certificate.file	<Vía de acceso>	Ubicación del archivo de certificado de cliente.	N
com.collation. bigfix.certificate.pwd	<Contraseña>	Contraseña del certificado de cliente.	N

4. BD del servidor de BigFix

Tabla 53.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.db.type	MSSQL o DB2	Tipo de BD que utiliza el servidor de BigFix; MSSQL para el servidor de BigFix basado en Windows o DB2 para el basado en Linux.	S
com.collation. bigfix.db.host	IP o FQDN	IP o FQDN de la BD de BigFix.	S
com.collation. bigfix.db.port	<núm. de puerto>	Puerto en el que TADDM se conectará con la base de datos de BigFix.	S
com.collation. bigfix.db.dbname	<nombre bd>	Nombre de la base de datos de BigFix.	S
com.collation. bigfix.db.domain	<dominio usuario>	Dominio de usuario: obligatorio en caso de que la autenticación esté basada en Windows.	N
com.collation. bigfix.db.domain	<IDusuario>	ID de usuario para acceder a la BD de BigFix.	S

Tabla 53. (continuación)

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.db.pwd	<contraseña>	Contraseña para acceder a la base de datos de BigFix; se almacenará en formato cifrado.	S

3. Consulte los registros de servidor de BigFix y la consola de BigFix para saber si existe algún estado de anomalía.

Nota:

- En caso de interrupción de la conexión entre TADDM y la base de datos, TADDM intentará volver a conectarse de acuerdo con el parámetro “com.collation.bigfix.result.wait”.
- En caso de cualquier cambio en los valores anteriores, se requiere el reinicio de TADDM.

5. TADDM: hebra de proceso/captación resultantes

Tabla 54.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.result.wait	<valor en segundos> Predeterminado=60 s	Cuando se habilita "com.collation.bigfix.enabled", se generará la hebra de captación de resultados para captar periódicamente los archivos resultantes de descubrimiento del servidor de BigFix. La “hebra de captación de resultados” captará los paquetes resultantes del servidor de BigFix según la periodicidad configurada (definida en segundos).	N
com.ibm.cdb. discover.asd. autodiscovery.enabled	True/false	Si es true, se habilitará la hebra para procesar los archivos resultantes de ASD almacenados.	S
com.ibm.cdb. discover.asd. ProcessUnreachableIPs	True/false	La hebra procesará el resultado de ASD para el destino que sea inalcanzable.	S
com.ibm.cdb. discover.asd. AsyncDiscovery ResultsDirectory	Vía de acceso predeterminada = var/asdd	Vía de acceso donde se conservan los archivos resultantes. La vía de acceso es configurable, pero se establece en var/asdd de forma predeterminada.	N
com.ibm.cdb. discover.asd. autodiscovery. asdScope	<nombre de ámbito> Predeterminado = ASD	La hebra seleccionará el destino mencionado en este ámbito para procesar el archivo resultante. Si esta propiedad no se menciona, se procesa el ámbito de ASD de forma predeterminada.	N

Tabla 54. (continuación)

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.ibm.cdb.discover.asd.autodiscovery.asdProfile	<nombre de perfil> Predeterminado = ASD	La hebra seleccionará los sensores mencionados en este perfil para procesar el archivo resultante. Si esta propiedad no se menciona, se procesa el perfil de ASD de forma predeterminada.	N
com.ibm.cdb.discover.asd.autodiscovery.filesThreshold	<umbral de archivos> Predeterminado=20	Número mínimo de archivos necesarios para el inicio de proceso de la hebra. La hebra procesará el resultado si se cumple el umbral de archivos o el umbral de tiempo.	N
com.ibm.cdb.discover.asd.autodiscovery.timeThreshold	<umbral de tiempo> Predeterminado=60s	Umbral de tiempo después del que la hebra procesará los archivos resultantes, incluso si no se cumple el umbral de archivos.	N

Nota: 1. Los resultados del descubrimiento de BigFix llegarán de forma asíncrona al servidor de TADDM, y siempre que se cumpla una de las propiedades (com.ibm.cdb.discover.asd.autodiscovery.filesThreshold, com.ibm.cdb.discover.asd.autodiscovery.timeThreshold) se procesará el grupo de archivos resultantes disponibles; esto creará una nueva entrada "Historial de descubrimientos". Estas propiedades se ajustarán según los requisitos específicos para controlar el número de entradas del "Historial de descubrimientos".

6. Limpieza

Tabla 55.

Núm.S	Recursos	Servidor de TADDM		Servidor raíz de BES		Punto final de BES	
		Creado	Limpieza	Creado	Limpieza	Creado	Limpieza
1.	Paquete de solicitudes	S	N[1]	S	N[2]	S	S
2.	Tarea	-	-	S	S [4]	-	-
3.	Acción	-	-	S	S [3]	-	-
4.	Paquete resultante	S	S	S	S	S	S
5.	Conjunto de archivos	-	-	-	-	S	S

Nota:

- No se da soporte a la limpieza de paquetes de solicitudes en el servidor de TADDM.
- No se da soporte a la limpieza de paquetes de solicitudes en el servidor raíz de BES. (El paquete de solicitudes se puede volver a utilizar durante el redescubrimiento).

- Solo se tendrán en cuenta para la limpieza las acciones creadas por TADDM y que están en estado Caducado (excepto para la acción creada con el nombre TADDMCLEANUP).
- Las tareas creadas por TADDM se eliminarán, solo cuando todas las acciones asociadas a dicha tarea ya se hayan eliminado.
- Las tareas creadas por TADDM se eliminarán, solo cuando todas las acciones asociadas a dicha tarea ya se hayan eliminado.
  – Para excluir una tarea específica y sus acciones asociadas de la limpieza (para el soporte de redescubrimiento), se puede utilizar retainBigFixTask.sh/.bat como se detalla a continuación:

  Uso: ./retainBigFixTask.sh <NombreTarea> <enable/disable>

Limpieza en el servidor de TADDM

Tabla 56.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.taddm. cleanup.volume	<tamaño límite con sufijo>	<Tamaño límite después del cual se eliminarán los archivos procesados antiguos, p. ej. 50MB, 2GB, etc.>	N
com.collation. bigfix.taddm. cleanup.time	<tiempo límite con sufijo>	<Para comprobar los archivos procesados más antiguos que las unidades configuradas, por ejemplo, 1D, 5H, 30M, etc.>	N
com.collation. bigfix.taddm. cleanup.runtime	Núm. de minutos	La hebra de limpieza de TADDM esperará el número de minutos configurado después de la ejecución.	N

Nota:

- Se efectuará la limpieza de los archivos resultantes en el servidor de TADDM, solo cuando se haya configurado como mínimo una de las propiedades (com.collation.bigfix.taddm.cleanup.volume, com.collation.bigfix.taddm.cleanup.time).

Limpieza en punto final

Tabla 57.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.endpoint. cleanup	<S o N> <Predeterminado=S>	Cuando se establece en S, se eliminarán del punto final el paquete de solicitudes comprimido, el directorio del paquete de solicitudes extraído y el paquete resultante comprimido recién creado.	N

Limpieza en el servidor raíz de BigFix

Tabla 58.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.root. cleanup.interval	<núm. de días> <Predeterminado=1>	Periodicidad de la ejecución de la tarea de limpieza para eliminar paquetes resultantes, tareas y acciones caducadas del servidor raíz de BES.	N
com.collation. bigfix.root. cleanup.days	<núm. de días> <Predeterminado=5>	Los archivos resultantes anteriores al número de días determinado se tendrán en cuenta para su eliminación.	N

7. Lenguaje de relevancia personalizado

Tabla 59.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.relevance. appendscope	true/false <Predeterminado=true>	Si es true, se utilizará la consulta de relevancia personalizada, además del ámbito especificado. Si es false, solo se utilizará la consulta de relevancia personalizada, en lugar del ámbito especificado.	N
com.collation. bigfix. relevance	True/false	Consulta de relevancia para identificar un conjunto de puntos finales para el descubrimiento dado.	N

8. Valores de vía de acceso temporal de paquete de BigFix

Tabla 60.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.action. enable.os	<script de acción para el SO configurado><Predeterminado=Windows, AIX, Linux, SunOS>	El script de acción para el SO configurado se incluirá en el lenguaje de scripts de acción de BigFix.	N
com.collation. bigfix.temp. Windows	Vía de acceso del paquete de solicitudes<Predeterminado=C:\Windows\ Temp>	La vía de acceso que se utilizará para el paquete de solicitudes de ASD. *Nota: sería necesario que "\" se indicara como "\\" en la vía de acceso de Windows.	N
com.collation. asd.temp.Windows	Vía de acceso del paquete resultante<Predeterminado=C:\Windows\ Temp>	La vía de acceso que se utilizará para los paquetes resultantes de ASD.	N

Tabla 60. (continuación)

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. asd.temp.Unix	Vía de acceso del paquete resultante<Predeterminado= /tmp>	La vía de acceso que se utilizará para el paquete resultante de ASD.	N
com.collation. bigfix.temp.Linux	Vía de acceso de paquete resultante <Predeterminado=/ tmp >	La vía de acceso que se utilizará para el paquete de solicitudes de ASD.	N
com.collation. bigfix.temp. SunOS	Vía de acceso del paquete resultante<Predeterminado= /tmp>	La vía de acceso que se utilizará para el paquete de solicitudes de ASD.	N
com.collation. bigfix.temp. AIX	Vía de acceso del paquete resultante<Predeterminado= /tmp>	La vía de acceso que se utilizará para el paquete de solicitudes de ASD.	N

Nota: Basándose en la vía de acceso temporal configurada anteriormente, la carpeta se creará en los puntos finales de destino, si no existe. Por ejemplo, en el caso de Windows 2003, se utilizará la vía de acceso temporal predeterminada " C:\Windows\Temp \" y esta carpeta se creará durante el descubrimiento.

Apéndice B. Ayuda de parámetros de script para diferentes modalidades

./runBigFixDiscovery.sh: herramienta de TADDM para la ejecución de un descubrimiento de BigFix mejorado o para consultar una acción de descubrimiento existente.

Modalidad: DESCUBRIMIENTO

Uso: bin/runBigFixDiscovery.sh -d/--discover [-c <arg>] [-freq <arg>] [-h] [-intr <arg>] -o <arg> -p <arg> -s <arg>

donde,

Tabla 61.

-c,--compressMethod <arg>	[Predeterminado: ZIP] Valores posibles: [ZIP, TAR].
-freq,--frequency <arg>	[Predeterminado: 1] Número de veces que debe ejecutarse el descubrimiento.
-h,--help	Se muestra la ayuda.
-intr,--interval <arg>	[Predeterminado: P1D] Intervalo de tiempo entre ejecuciones de descubrimiento. Valores admitidos: [PT15M, PT30M, PT1H, PT2H, PT4H, PT6H, PT8H, PT12H, P1D, P2D, P3D, P5D, P7D, P15D, P30D].
-o,--output <arg>	NECESARIO: directorio de salida donde se generará el paquete de descubrimiento de BigFix.

Tabla 61. (continuación)

-p,--profile <arg>	NECESARIO: el nombre de perfil que se utilizará en la creación del paquete de descubrimiento para incluir los sensores.
-s,--scope	NECESARIO: nombres de ámbito/grupo de ámbitos. (Separados por comas. Incluya entre comillas los nombres que contengan espacios).

Modalidad: SONDEO

Uso: bin/runBigFixDiscovery.sh -p/--poll [-h] -i <arg> [-r <arg>] [-t <arg>]

donde,

Tabla 62.

-d,--detail <arg>	[Predeterminado: true] Resultado de sondeo para cada punto final.
-h,--help	Se muestra la ayuda.
-r,--repeat <arg>	[Predeterminado: 1] Número de veces que debe sondearse el estado de la acción.
-i,--id <arg>	NECESARIO: ID de la acción que se va a sondear.
-t,--timeout <arg>	[Predeterminado: 1] Intervalo entre SONDEOS consecutivos en segundos.

Modalidad: LIMPIEZA

Uso: bin/runBigFixDiscovery.sh -c/--cleanup [-d <arg>] [-h]

donde,

Tabla 63.

-h,--help	Se muestra la ayuda.
-d,--days <arg>	[Predeterminado: 5] Se limpian los archivos resultantes anteriores al número de días especificado.

Modalidad: REDESCUBRIMIENTO

Uso: bin/runBigFixDiscovery.sh -r/--rediscover [-freq <arg>] [-h] [-intr <arg>]

donde,

Tabla 64.

-freq,--frequency <arg>	[Predeterminado: 1] Número de veces que debe ejecutarse el descubrimiento.
-h,--help	Se muestra la ayuda.

Tabla 64. (continuación)

-intr,--interval <arg>	[Predeterminado: P1D] Intervalo de tiempo entre ejecuciones de descubrimiento. Valores admitidos: [PT15M, PT30M, PT1H, PT2H, PT4H, PT6H, PT8H, PT12H, P1D, P2D, P3D, P5D, P7D, P15D, P30D].

5. TADDM: hebra de proceso/captación resultantes

Tabla 65.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.result.wait	<valor en segundos> Predeterminado=60 s	Cuando se habilita "com.collation.bigfix.enabled", se generará la hebra de captación de resultados para captar periódicamente los archivos resultantes de descubrimiento del servidor de BigFix. La “hebra de captación de resultados” captará los paquetes resultantes del servidor de BigFix según la periodicidad configurada (definida en segundos).	N
com.ibm.cdb. discover.asd. autodiscovery. enabled	True/false	Si es true, se habilitará la hebra para procesar los archivos resultantes de ASD almacenados.	S
com.ibm.cdb. discover.asd. ProcessUnreachableIPs	True/false	La hebra procesará el resultado de ASD para el destino que sea inalcanzable.	S
com.ibm.cdb. discover.asd. AsyncDiscovery ResultsDirectory	Vía de acceso predeterminada = var/asdd	Vía de acceso donde se conservan los archivos resultantes. La vía de acceso es configurable, pero se establece en var/asdd de forma predeterminada.	N
com.ibm.cdb. discover.asd. autodiscovery. asdScope	<nombre de ámbito> Predeterminado = ASD	La hebra seleccionará el destino mencionado en este ámbito para procesar el archivo resultante. Si esta propiedad no se menciona, se procesa el ámbito de ASD de forma predeterminada.	N
com.ibm.cdb. discover.asd. autodiscovery. asdProfile	<nombre de perfil> Predeterminado = ASD	La hebra seleccionará los sensores mencionados en este perfil para procesar el archivo resultante. Si esta propiedad no se menciona, se procesa el perfil de ASD de forma predeterminada.	N

Tabla 65. (continuación)

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.ibm.cdb.discover.asd.autodiscovery.filesThreshold	<umbral de archivos> Predeterminado=20	Número mínimo de archivos necesarios para el inicio de proceso de la hebra. La hebra procesará el resultado si se cumple el umbral de archivos o el umbral de tiempo.	N
com.ibm.cdb.discover.asd.autodiscovery.timeThreshold	<umbral de tiempo> Predeterminado=60 s	Umbral de tiempo después del que la hebra procesará los archivos resultantes, incluso si no se cumple el umbral de archivos.	N

Nota: 1. Los resultados del descubrimiento de BigFix llegarán de forma asíncrona al servidor de TADDM, y siempre que se cumpla una de las propiedades (com.ibm.cdb.discover.asd.autodiscovery.filesThreshold, com.ibm.cdb.discover.asd.autodiscovery.timeThreshold) se procesará el grupo de archivos resultantes disponibles; esto creará una nueva entrada "Historial de descubrimientos". Estas propiedades se ajustarán según los requisitos específicos para controlar el número de entradas del "Historial de descubrimientos".

6. Limpieza

Tabla 66.

Núm.S	Recursos	Servidor de TADDM		Servidor raíz de BES		Punto final de BES	
		Creado	Limpieza	Creado	Limpieza	Creado	Limpieza
1.	Paquete de solicitudes	S	N[1]	S	N[2]	S	S
2.	Tarea	-	-	S	S [4]	-	-
3.	Acción	-	-	S	S [3]	-	-
4.	Paquete resultante	S	S	S	S	S	S
5.	Conjunto de archivos	-	-	-	-	S	S

Nota:

- No se da soporte a la limpieza de paquetes de solicitudes en el servidor de TADDM.
- No se da soporte a la limpieza de paquetes de solicitudes en el servidor raíz de BES. (El paquete de solicitudes se puede volver a utilizar durante el redescubrimiento).
- Solo se tendrán en cuenta para la limpieza las acciones creadas por TADDM y que están en estado Caducado (excepto para la acción creada con el nombre TADDMCLEANUP).
- Las tareas creadas por TADDM se eliminarán, solo cuando todas las acciones asociadas a dicha tarea ya se hayan eliminado.
- Las tareas creadas por TADDM se eliminarán, solo cuando todas las acciones asociadas a dicha tarea ya se hayan eliminado.

– Para excluir una tarea específica y sus acciones asociadas de la limpieza (para el soporte de redescubrimiento), se puede utilizar retainBigFixTask.sh/.bat como se detalla a continuación:

Uso: ./retainBigFixTask.sh <NombreTarea> <enable/disable>

Limpieza en el servidor de TADDM

Tabla 67.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation.bigfix.taddm.cleanup.volume	<tamaño límite con sufijo>	<Tamaño límite después del cual se eliminarán los archivos procesados antiguos, p. ej. 50MB, 2GB, etc.>	N
com.collation.bigfix.taddm.cleanup.time	<tiempo límite con sufijo>	<Para comprobar los archivos procesados más antiguos que las unidades configuradas, por ejemplo, 1D, 5H, 30M, etc.>	N
com.collation.bigfix.taddm.cleanup.runtime	Núm. de minutos	La hebra de limpieza de TADDM esperará el número de minutos configurado después de la ejecución.	N

Nota:

- Se efectuará la limpieza de los archivos resultantes en el servidor de TADDM, solo cuando se haya configurado como mínimo una de las propiedades (com.collation.bigfix.taddm.cleanup.volume, com.collation.bigfix.taddm.cleanup.time).

Limpieza en punto final

Tabla 68.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation.bigfix.endpoint.cleanup	<S o N><Predeterminado=S>	Cuando se establece en S, se eliminarán del punto final el paquete de solicitudes comprimido, el directorio del paquete de solicitudes extraído y el paquete resultante comprimido recién creado.	N

Limpieza en el servidor raíz de BigFix

Tabla 69.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation.bigfix.root.cleanup.interval	<núm. de días> <Predeterminado=1>	Periodicidad de la ejecución de la tarea de limpieza para eliminar paquetes resultantes, tareas y acciones caducadas del servidor raíz de BES.	N

Tabla 69. (continuación)

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation.bigfix.root.cleanup.days	<núm. de días> <Predeterminado=5>	Los archivos resultantes anteriores al número de días determinado se tendrán en cuenta para su eliminación.	N

7. Lenguaje de relevancia personalizado

Tabla 70.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation.bigfix.relevance.appendscope	true/false <Predeterminado=true>	Si es true, se utilizará la consulta de relevancia personalizada, además del ámbito especificado. Si es false, solo se utilizará la consulta de relevancia personalizada, en lugar del ámbito especificado.	N
com.collation.bigfix.relevance	True/false	Consulta de relevancia para identificar un conjunto de puntos finales para el descubrimiento dado.	N

8. Valores de vía de acceso temporal de paquete de BigFix

Tabla 71.

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation.bigfix.action.enable.os	<script de acción para el SO configurado> <Predeterminado=Windows, AIX, Linux, SunOS>	El script de acción para el SO configurado se incluirá en el lenguaje de scripts de acción de BigFix.	N
com.collation.bigfix.temp.Windows	Vía de acceso del paquete de solicitudes <Predeterminado=C:\Windows\Temp>	La vía de acceso que se utilizará para el paquete de solicitudes de ASD. *Nota: sería necesario que "\" se indicara como "\\" en la vía de acceso de Windows.	N
com.collation.asd.temp.Windows	Vía de acceso del paquete resultante <Predeterminado=C:\Windows\Temp>	La vía de acceso que se utilizará para los paquetes resultantes de ASD.	N
com.collation.asd.temp.Unix	Vía de acceso de paquete resultante <Predeterminado=/tmp>	La vía de acceso que se utilizará para el paquete resultante de ASD.	N
com.collation.bigfix.temp.Linux	Vía de acceso de paquete resultante <Predeterminado=/tmp>	La vía de acceso que se utilizará para el paquete de solicitudes de ASD.	N

Tabla 71. (continuación)

Nombre de propiedad	Valores posibles	Descripción	Obligatorio
com.collation. bigfix.temp. SunOS	Vía de acceso de paquete resultante <Predeterminado=/tmp >	La vía de acceso que se utilizará para el paquete de solicitudes de ASD.	N
com.collation. bigfix.temp. AIX	Vía de acceso de paquete resultante <Predeterminado=/tmp >	La vía de acceso que se utilizará para el paquete de solicitudes de ASD.	N

Nota: Basándose en la vía de acceso temporal configurada anteriormente, la carpeta se creará en los puntos finales de destino, si no existe. Por ejemplo, en el caso de Windows 2003, se utilizará la vía de acceso temporal predeterminada " C:\Windows\Temp \" y esta carpeta se creará durante el descubrimiento.

Apéndice C. Ejemplo de comprobación de la ejecución de scripts

1. Ejecución de script: encryptprops.sh

```
/opt/IBM/taddm/dist/bin/encryptprops.sh $COLLATION_HOME
```

2. Ejecución de script: runBigFixDiscovery.sh

```
TADDM Server  – 9.167.42.227 (Linux)
BigFix server     – 10.160.161.195 (windows)
BigFix endpoints        – 10.160.161.196 (windows)
                           10.160.161.212 (windows)
Scope       – ASD (con ambos puntos finales de BigFix)
Profile           - ASD (con los sensores mencionados en la sección 2.2)
Configuration     - según se describe en la sección 3.
```

a. Inicio del descubrimiento:

```
[taddmusr@nc042227 bin]$ ./runBigFixDiscovery.sh -d -o /tmp -p ASD -s ASD
BigFix Action will be applied total [1] times with [P1D] interval

Task created on BES server with Name [20170828083852] and Action created with ID [633]

DISCOVER: LAUNCH OK
The Bigfix Discovery script exited successfully.
```

b. Nombre de tarea: 20170828083852, ID de acción: 633

c. Inicio de sondeo:

```
[taddmusr@nc042227 bin]$ ./runBigFixDiscovery.sh -p -i 633
Repeatedly poll the BigFix Action [1] number of times for every [1] seconds
Total [2] Computers returned for Action with ID [633] has status: Open

Total [1] computers with status : The action executed successfully.
[Hostname] [Apply Count] [Line Number] [Start Time] [End Time]
[PNC161196] [1] [98] [Mon, 28 Aug 2017 14:43:56 +0000] [Mon, 28 Aug 2017 14:44:11 +0000]

Total [1] computers with status : The action failed.
[Hostname] [Apply Count] [Line Number] [Start Time] [End Time]
[PRODUCTIONWASB] [1] [37] [Mon, 28 Aug 2017 07:40:26 +0000] [Mon, 28 Aug 2017 07:40:26 +0000]

POLL FINISHED
The Bigfix Discovery script exited successfully
```

Inicio de limpieza:

```
[taddmusr@nc042227 bin]$ ./runBigFixDiscovery.sh -c
CLEANUP TASK FOUND: TADDMCLEANUP with ID: 2067

Cleanup Action created with ID: [2068]

CLEANUP: LAUNCH OK
The Bigfix Discovery script exited successfully
```

Inicio de redescubrimiento:

```
[taddmusr@nc042227 bin]$ ./runBigFixDiscovery.sh –r –i 20171117085907

TASK FOUND : 20171117085907 with ID : 2075

Action created with ID: [2086]

REDISCOVERY: LAUNCH OK
The Bigfix Discovery script exited successfully.
```

Apéndice D. Códigos de error y descripción

Tabla 72.

ID de mensaje	M:Mensaje, C:Causa, E:Efecto
CTJTD1260E	M: El descubrimiento de Bigfix no está habilitado. Configure com.collation.bigfix.enabled en collation.properties E: El script de descubrimiento de Bigfix no se ejecutará y no se invocará la hebra para captar el resultado
CTJTD1261E	M: Faltan argumentos o son incorrectos C: Intente ejecutar el script con una modalidad distinta de Descubrir, Sondear, Limpiar o Redescubrir E: El script no se ejecutará
CTJTD1262E	M: Se ha proporcionado un formato de número incorrecto C: Las propiedades o los argumentos se han especificado en formato de cadena y no de número E: El script de descubrimiento de Bigfix no se ejecutará y no funcionará la hebra para captar el resultado
CTJTD1263E	M: No se han podido analizar las propiedades de la línea de mandatos: <nombre de propiedad> C: Se han pasado los argumentos mientras no se da soporte a la ejecución de los scripts E: No se invocará la modalidad de scripts
CTJTD1264E	M: Falta <nombre de propiedad> en collation.properties C: En la ejecución de script faltan propiedades necesarias o estas no son válidas (consulte el Apéndice A) E: El script de descubrimiento de Bigfix no se ejecutará y no funcionará la hebra para captar el resultado
CTJTD1265I	M: Solo se utilizará la relevancia personalizada, en lugar del ámbito especificado
CTJTD1266I	M: Se utilizará la relevancia personalizada, además del ámbito especificado

Tabla 72. (continuación)

ID de mensaje	M:Mensaje, C:Causa, E:Efecto
CTJTD1267E	M: Se ha especificado un ámbito vacío; no se han encontrado elementos C: El ámbito/grupo de ámbitos determinado no contiene ningún elemento para definir el punto final E: No se invocará el descubrimiento
CTJTD1268E	M: No hay sensores presentes o habilitados en el perfil especificado C: El perfil determinado no contiene sensores E: No se invocará el descubrimiento
CTJTD1269E	M: El paquete de solicitud AASD no existe C: Se ha producido un problema al crear el paquete de solicitud o este no tiene permiso o no existe para cargarlo E: No se invocará el descubrimiento
CTJTD1270E	M: El tamaño del paquete AASD es mayor que el umbral configurado en com.collation.bigfix.aasdpkgmaxsize C: El tamaño del paquete de solicitud creado es mayor que la configuración E: No se invocará el descubrimiento
CTJTD1271E	M: No se puede establecer la conexión con BigFix por la razón: <razón> C: Se ha producido un problema de conexión con el servicio web de Bigfix debido a parámetros no válidos o a un certificado no válido E: El paquete no se cargará y no se invocará el descubrimiento
CTJTD1272E	M: Capturado un error durante la configuración: <razón> C: Se ha producido un escenario inesperado para el código que no se puede manejar E: La ejecución del script no funcionará de forma apropiada
CTJTD1273I	M: Script principal para (re)ejecutar un descubrimiento de BigFix, O BIEN para SONDEAR una Acción de descubrimiento especificada o para realizar una limpieza manual

Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en EE. UU. Es posible que IBM no ofrezca los productos, los servicios o las funciones mencionados en otros países. Consulte a su representante local de IBM para obtener información sobre los productos y servicios disponibles actualmente en su área. Toda referencia a un producto, programa o servicio de IBM no implica que sólo pueda usarse un producto, programa o servicio de IBM. En su lugar puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ningún derecho de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de esos productos, programas o servicios que no son de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran temas descritos en este documento. La entrega de este documento no le garantiza licencias para dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 EE. UU.

Para consultas relativas a información de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM en su país o dirija sus consultas por escrito a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde tales disposiciones contradigan la legislación vigente:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA.

Algunos estados no permiten la renuncia de garantías explícitas o implícitas en determinadas transacciones, por lo que es posible que este párrafo no se aplique en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí incluida; dichos cambios se incorporarán en nuevas ediciones de esta publicación. IBM puede realizar mejoras y/o cambios en los productos y/o programas descritos en esta publicación cuando lo considere oportuno y sin previo aviso.

Todas las referencias que se hacen en esta información a sitios web no IBM son meramente informativas y en modo alguno representan una recomendación de dichos sitios web. El material de esos sitios web no forma parte del material de este producto de IBM y la utilización de esos sitios web se realizará bajo su total responsabilidad.

IBM se reserva el derecho de utilizar o distribuir, en la forma que considere más adecuada, la información que se le facilite sin incurrir por ello en ninguna obligación con el remitente.

Los titulares de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido este) y (ii) el uso compartido de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 EE.UU.

Puede que dicha información esté disponible, sujeta a los términos y condiciones adecuados, y puede incluir en algunos casos, el pago de una tarifa.

IBM proporciona el programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del Acuerdo del Cliente de IBM, el Acuerdo Internacional de Licencia de Programas de IBM o cualquier acuerdo equivalente entre las partes.

Todos los datos de rendimiento que contiene este documento se han determinado en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar de manera significativa. Algunas mediciones se han realizado en sistemas en desarrollo y no se garantiza que sean las mismas para sistemas disponibles en general. Además, alguna medición puede haberse estimado por extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información sobre los productos que no son de IBM se ha obtenido de los proveedores de dichos productos, sus declaraciones publicadas u otras fuentes públicas disponibles. IBM no ha probado esos productos, por lo que no puede confirmar la corrección de su rendimiento, su compatibilidad ni otras afirmaciones relacionadas con productos que no sean de IBM. Las preguntas sobre las posibilidades de los productos que no sean de IBM deben dirigirse a los proveedores de dichos productos.

Todas las declaraciones sobre la dirección o las intenciones futuras de IBM están sujetas a modificaciones o a retirada sin previo aviso, y representan sólo objetivos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones de empresa diarias. Para ilustrarlas de la mejor manera posible, en los ejemplos se incluyen nombres de personas, empresas, sucursales y productos. Todos estos nombres son ficticios, y cualquier parecido con nombres y direcciones utilizados por una empresa real son mera coincidencia.

Si está viendo esta información en formato de software, es posible que no aparezcan las fotografías ni las ilustraciones en color.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas de International Business Machines Corp., registrados en muchas jurisdicciones a nivel mundial. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. En el apartado “Copyright and trademark information” (información de copyright y marcas registradas) de la página web http://www.ibm.com/legal/copytrade.shtml encontrará una lista actualizada de las marcas registradas de IBM.

Java y todas las marcas comerciales y logotipos basados en Java son marcas comerciales o marcas registradas de Oracle y/o sus afiliadas.

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft y Windows son marcas comerciales de Microsoft Corporation en EE. UU. o en otros países.

UNIX es una marca comercial registrada de The Open Group en Estados Unidos y en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o de servicio de terceros.

Impreso en España